Directorate for Preparedness
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MEMORANDUM FOR: NIMS Stakeholders

FROM: Bob Shea
Assistant Deputy Director, FEMA

Tina Gabbrielli
Senior Director, Contingency Planning and Field Based Preparedness Division, NPTF

SUBJECT: First National Comment Period on Upgraded National Incident Management System

The Department of Homeland Security (DHS), is coordinating a comprehensive review of the National Response Plan (NRP) and National Incident Management System (NIMS) to assess their effectiveness and identify improvements. The review process, which includes participation from all levels of stakeholders, commenced in October 2006 and is scheduled to be concluded by June 1, 2007.

The NIMS is a key element in the national framework for domestic incident management. It provides a nationwide template that enables Federal, State, local and tribal governments, the private-sector and non-governmental organizations to work together efficiently and effectively to manage the consequences of domestic incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property.

As part of the review process, stakeholders will be asked to participate in two formal comment periods on both documents to ensure their effectiveness as national doctrine for incident management. Work groups representing all levels of stakeholders have been working diligently, under a very compressed timeframe, to develop a first draft of the NIMS document which we are releasing for national comment between February 1 – 19, 2007. Due to the tight time constraints, the work groups focused on resolving key concepts, rather than technical edits. As you review the document, please take this into account and concentrate on providing substantive vice administrative comments to the document. A technical edit will be conducted simultaneously during this review period.

If you would like to request a comment form to submit comments, please email NIMScomments@hsi.dhs.gov. However, while a comment form will help assure clarity and consistency, it is not a requirement. You may also submit your comments directly to that email address.

Your organization's participation in the NRP/NIMS review process is essential to ensure that the Nation can effectively and efficiently prepare for, prevent, respond to, and recover from any type of incident. Direct questions regarding the NIMS Upgrade Document can be forwarded to Mr. Al Fluman, Acting Director of the NIMS Integration Center at FEMA, at al.fluman@dhs.gov.

NATIONAL INCIDENT MANAGEMENT SYSTEM

February 1, 2007

Draft Note: This is a draft document; all alterations to the original document are represented in **Blue** font throughout the document. Original text is in **Black** font and has not been altered, although it may have been moved from its original location.

Commenting on the Draft Document: If you would like to submit comments on the DRAFT NIMS document email your comments to NIMScomments@hsi.dhs.gov OR send an email to request a comment form. Submitting comments using this form is NOT required but will help assure clarity and continuity during the comment adjudication process.

Working Papers: This document does not constitute an official re-release of the NIMS.

(This Page Intentionally Left Blank)

LETTER FROM SECRETARY OF THE DEPARTMENT OF HOMELAND SECURITY TO BE REVISED AND RE-INSERTED AT A LATER DATE

CONTENTS

CONTENTS

LIST OF TABLES AND FIGURES

CONTENTS

WHAT IS THE NATIONAL INCIDENT MANAGEMENT SYSTEM?

The National Incident Management System is a systematic, proactive approach guiding government agencies at all levels, private sector, and nongovernmental organizations to work seamlessly to efficiently and effectively prepare for, prevent, respond to, and recover from incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property.

PREFACE

On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD)–5, *Management of Incidents*, which directed the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS).[1] This National Incident Management System provides a consistent nationwide template to enable Federal, State, local, and Tribal governments and private sector and nongovernmental organizations to work together effectively and efficiently to prepare for, prevent, respond to, and recover from incidents, regardless of cause, size, or complexity, including acts of catastrophic terrorism. This consistency provides the foundation for utilization of the NIMS for all incidents, ranging from daily occurrences to incidents requiring a coordinated Federal response, including "Incidents of National Significance."

The NIMS represents a core set of doctrine, concepts, principles, terminology, and organizational processes that enables effective, efficient, and collaborative incident management at all levels. **It is not an operational incident management or resource allocation plan.** To this end, HSPD-5 required the Secretary of Homeland Security to develop the National Response Plan (NRP), which integrates Federal government prevention, preparedness, response, and recovery plans into a single, all-disciplines, all-hazards plan. The NRP, using the comprehensive framework provided by the NIMS, provides the structure and mechanisms for national-level policy and operational direction for Federal support to State, local and Tribal incident managers and for exercising direct Federal authorities and responsibilities as appropriate under the law.

HSPD-5 requires all Federal departments and agencies to adopt the NIMS and to use it in their individual incident management and emergency prevention, preparedness, response, recovery, and mitigation programs and activities, as well as in support of all actions taken to assist State, local, or Tribal entities. The directive required Federal departments and agencies to make adoption of the NIMS by State and local organizations a condition for Federal preparedness assistance (through grants, contracts, and other activities) beginning in Fiscal Year 2005. Jurisdictional compliance with certain aspects of the NIMS will be possible in the short term, such as adopting the basic tenets of the Incident Command System (ICS) identified in this document. Other aspects of the NIMS, however, will require additional development and refinement to enable compliance at a future date (e.g., data and communications systems interoperability).

Building on the foundation provided by existing incident management and emergency response systems used by jurisdictions and functional disciplines at all levels, the NIMS document integrates best practices

[1] FY2007 DHS Appropriations Bill, PL 109-295, Section 509. "SEC. 509. NATIONAL INTEGRATION CENTER. (a) In General.—There is established in the Agency a National International Center. (b) Responsibilities.— (1) In General.—The Administrator, through the National Integration Center, and in consultation with other Federal departments and agencies and the National Advisory Council, shall ensure ongoing management and maintenance of the National Incident Management System, the National Response Plan and any successor to such system or plan."

into a comprehensive framework for use by incident management organizations in an all-hazards context nationwide. These best practices lay the groundwork for the components of the NIMS and provide the mechanisms for the further development and refinement of supporting national standards, guidelines, protocols, systems, and technologies. The NIMS fosters the development of specialized technologies that facilitate incident management and allows for the adoption of new approaches that will enable continuous refinement of the NIMS over time.

The Secretary of Homeland Security, through the NIMS Integration Center (NIC) discussed in the Ongoing Management and Maintenance section, will publish separately the standards, guidelines, and compliance protocols for determining whether a Federal, State, local, or Tribal entity has adopted the aspects of the NIMS that are in place by October 1, 2004. The Secretary, through the NIC, will also publish, on an ongoing basis, additional standards, guidelines, and compliance protocols for the aspects of the NIMS not yet fully developed.

This document was developed through a collaborative, inter-governmental partnership with significant input from the incident management functional disciplines, the private sector, and nongovernmental organizations. Originally published on March 1, 2004, the document was upgraded in 2007 to reflect contributions from stakeholders and lessons learned during recent incidents.

INTRODUCTION AND OVERVIEW

INTRODUCTION

The September 11, 2001, attacks and the 2004 and 2005 hurricane seasons highlighted the need to focus on improving prevention, preparedness, response, recovery, and mitigation capabilities and coordination processes across the country. A comprehensive national approach to incident management, applicable at all jurisdictional levels and across functional disciplines, would further improve the effectiveness of emergency response providers[2] and incident management organizations across a full spectrum of potential incidents and hazard scenarios. Such an approach would also improve coordination and cooperation between public and private entities in a variety of incident management activities.[3]

On February 28, 2003, the President issued a Homeland Security Presidential Directive –5, *Management of Domestic Incidents*, which directed the Secretary of Homeland Security to develop and administer a NIMS the purpose of which is to:

[2] As defined in the Homeland Security Act of 2002, Section 2(6), "The term 'emergency response providers' includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities." 6 U.S.C. section 101(6).

[3] For purposes of this document, incidents can include acts of terrorism, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, typhoons, war-related disasters, etc.

> [P]rovide a consistent nationwide approach for Federal, State,[4] and local[5] governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.[6]

While most incidents are generally handled on a daily basis by a single jurisdiction at the local level, there are important instances in which successful incident management operations depend on the involvement of multiple jurisdictions, functional agencies, and emergency responder disciplines. These instances require effective and efficient coordination across this broad spectrum of organizations and activities. The NIMS uses a systems approach to integrate the best existing processes and methods into a unified national framework for incident management. This framework forms the basis for interoperability and compatibility that will, in turn, enable a diverse set of public and private organizations to conduct well-integrated and effective incident management operations. It does this through a core set of concepts, principles, procedures, organizational processes, terminology, and standards requirements applicable to a broad community of NIMS users.

---

[4] As defined in the Homeland Security Act of 2002, the term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. 6 U.S.C. section 101(14).

[5] As defined in the Homeland Security Act of 2002, Section 2(10), the term," local government" means "(A) county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or inter-state government entity, or agency or instrumentality of a local government; an Indian tribe or authorized Tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity." 6 U.S.C. section 101(10).

[6]Homeland Security Presidential Directive/HSPD–5: Management of Domestic Incidents. The White House, Office of the Press Secretary. February 2003. http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html.

Table 1—Overview of the NIMS

What the NIMS is:	What the NIMS is NOT:
• A comprehensive nationwide systematic approach to incident management to include: ICS, MACS and PIS	• A response plan
• Set of preparedness concepts and principles for all hazards	• Only used during Incidents of National Significance
• Essential principles for a common operating picture and interoperability of communications and information management	• A communication plan
• Standardized resource management procedures that enable coordination among different jurisdictions or organizations	• Only applicable to certain emergency responders
• Scalable so it may be used for all incidents (from day-to-day to large-scale)	• Only the Incident Command System
• An evolutionary system that promotes ongoing management and maintenance	• A static system

CONCEPTS AND PRINCIPLES

The central tenets of the NIMS provide a framework for interoperability and compatibility, and maintain a balance between flexibility and standardization. The NIMS is flexible because the system components can be utilized to develop plans, processes, procedures, agreements and roles for all types of incidents and is applicable to any incident regardless of cause, size, location, or complexity. The flexibility and standardization within the NIMS is realized during an incident when organizations have previously coordinated and practiced using these tools.

FLEXIBILITY

The NIMS components are adaptable to any situation from small, local events to incidents requiring coordinated response, including Incidents of National Significance, whether pre-planned (e.g. structure used to manage major sporting or community events), notice, or no-notice. This flexibility is essential for the NIMS to be applicable across the full spectrum of multi-agency, multi-jurisdiction, and multi-discipline events. Flexibility in the NIMS framework facilitates scalability of incident management.

STANDARDIZATION

Flexibility of incident management requires coordination and standardization among responders and organizations whose incident management activities are based on a common framework. The NIMS provides a set of standardized organizational structures that improve integration and connectivity among jurisdictions and disciplines, starting with a common foundation of preparedness and planning. Personnel and organizations that have adopted the common NIMS framework are able to work together effectively and efficiently, thereby fostering cohesion among the various organizations involved in all stages of an incident. The NIMS also provides standard terminology which fosters more effective communication among agencies and organizations responding together to an incident.

OVERVIEW

The NIMS integrates existing best practices into a consistent, nationwide systems approach to incident management that is applicable at all government levels, nongovernmental organizations (NGO), private sector, and across functional disciplines in an all-hazards context. Four major components make up this systems approach: Preparedness, Communications and Information Management, Resource Management, and Command & Management.

NIMS COMPONENTS

The NIMS components were not designed to stand alone. The components work together as a system to provide the national framework for incident management. Similar to a table with four legs which will collapse if one of the legs is missing, the NIMS does not yield optimal results when one of its "legs" is absent. A more detailed discussion of each component is included in subsequent sections of this document.

PREPAREDNESS

Effective incident management begins with a host of preparedness activities conducted on a "steady-state" basis, well in advance of any potential incident. Preparedness involves an integrated combination of planning, training, exercising, and organizing qualified and/or credentialed personnel and standardized equipment.

COMMUNICATIONS AND INFORMATION MANAGEMENT

Incident response and management rely upon communications and information systems that provide a common operating picture to all command and coordination sites. The NIMS describes the requirement for a standardized framework for communications, information management (collection, analysis, and dissemination), and information-sharing at all levels of incident management.

RESOURCE MANAGEMENT

Incident managers need resources to support critical incident objectives. The flow of resources must be fluid and adaptable to the requirements of the incident. The NIMS defines standardized mechanisms and establishes requirements for processes to describe, inventory, mobilize, dispatch, track, and recover resources over the life-cycle of an incident.

COMMAND AND MANAGEMENT

The Command and Management system within the NIMS is designed to enable effective and efficient incident management and coordination by providing standardized incident management structures. The structure is based on three key organizational systems: (1) the Incident Command System, (2) Multi-agency Coordination Systems, and (3) the Public Information System.

ONGOING MANAGEMENT AND MAINTENANCE

HSPD-5 required the Secretary of Homeland Security to establish a mechanism for ensuring the ongoing management and maintenance of the NIMS.[7] Within the auspices of Ongoing Management and

[7] FY2007 DHS Appropriations Bill, PL 109-295, Section 509. "SEC. 509. NATIONAL INTEGRATION CENTER. (a) In General.—There is established in the Agency a National International Center. (b) Responsibilities.— (1) In General.—The Administrator, through the National Integration Center, and in consultation with other Federal departments and agencies and the National Advisory Council, shall ensure ongoing management and maintenance of the National Incident Management System, the National Response Plan and any successor to such system or plan."

Maintenance there are two components: The NIMS Integration Center (NIC), and Supporting Technologies.

NIMS INTEGRATION CENTER

The NIMS Integration Center provides strategic direction, oversight, and coordination of the NIMS. The NIC supports both routine maintenance and the continuous refinement of the NIMS and its components over the long term.

The NIC oversees and coordinates all aspects of the NIMS including the development of compliance criteria and implementation activities at Federal, State, Tribal and local levels. It provides guidance and support to jurisdictions and incident-management and responder organizations as they adopt the system.[8]

SUPPORTING TECHNOLOGIES

As the NIMS and its supporting systems evolve to be ever more flexible, scalable, and reliable, incident managers and those in coordinating roles will increasingly rely upon new technology and systems to implement and continuously refine the NIMS. The NIC oversees and coordinates the ongoing development of science and technology, which is integral to continual improvement and refinement of the NIMS including strategic research and development (R&D), to ensure that this development takes place.

[8] The NIC also provides information on available classes and training material on its website. For more information see: http://www.fema.gov/emergency/nims/index.shtm.

COMPONENT I

PREPAREDNESS

If faced with an incident or the threat of an impending incident, are emergency management policies, plans, procedures, trained personnel, and equipment ready to take immediate action to effectively prevent, protect against, respond to, and recover from the threat or incident? To answer "yes" to this question, a jurisdiction must have comprehensive preparedness efforts underway.

Preparedness involves an integrated combination of planning, training, exercises, personnel qualification and certification standards, and equipment certification standards. A major objective of preparedness efforts is to ensure mission integration and interoperability in response to emergent crises across functional and jurisdictional lines, as well as between public and private organizations. Adequate preparedness enables efficient and effective incident management.

This component describes specific measures and capabilities that jurisdictions and agencies should develop and incorporate into an overall risk reduction strategy to enhance operational preparedness for incident management on a steady-state basis in an all-hazards context.[9] In developing, refining, and expanding preparedness programs and activities within their jurisdictions and organizations, incident management officials should leverage existing preparedness efforts and collaborative relationships to the greatest extent possible.

CONCEPTS AND PRINCIPLES

Under the NIMS, preparedness is based on the following core concepts and principles: (1) Levels of Capability, (2) A Unified Approach, and (3) Mitigation and Risk Reduction.

[9] The operational preparedness of our nation's incident management capabilities is distinct from the preparedness of individual citizens and private industry. Public preparedness for domestic incidents is beyond the scope of the NIMS but is an important element of homeland security. Websites such as: www.ready.gov, provide further information on community preparedness.

LEVELS OF CAPABILITY

Preparedness involves actions to establish and to sustain prescribed levels of capability necessary to execute a full range of incident management activities. Preparedness is implemented through a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking action to correct and mitigate. Within the NIMS, preparedness focuses on guidelines, protocols, and standards for planning, training, personnel qualification and certification, and equipment certification. Publication management also supports all aspects of preparedness and is managed by the NIC.[10]

A UNIFIED APPROACH

Preparedness requires a unified approach. A major objective of preparedness efforts is to ensure mission integration and interoperability in response to emergent crises across functional and jurisdictional lines, as well as between public and private organizations.

MITIGATION AND RISK REDUCTION

Mitigation and risk reduction activities are important elements of preparedness and provide a critical foundation across the incident management spectrum from prevention through response and recovery by breaking the cycle of disaster damage, reconstruction, and repeated damage. Mitigation is the effort to reduce the loss of life and property by lessening the impact of disasters and provides value to the public by creating safer communities and reducing loss of life and property.

Risk reduction is the effort to minimize the risk to life and property (including future construction and existing structures) in the pre-incident and post-incident environments. Risk reduction is achieved through means such as regulations, ordinances, land use planning, public education, and building codes. Examples of mitigation and risk reduction activities include the following:

- ongoing public education and outreach activities designed to reduce loss of life and destruction of property;
- complying with or exceeding the National Flood Insurance Program (NFIP) floodplain management regulations;
- enforcing stringent building codes, flood-proofing requirements, seismic design standards and wind-bracing requirements for new construction or repairing existing buildings;
- retrofitting public buildings to withstand hurricane-strength winds or ground shaking;
- supporting measures to ensure the protection and resilience of critical infrastructure and key resources designed to ensure continuity of business and the economic stability of communities;

[10] See page 81. Ongoing Management and Maintenance, *NIMS Integration Center.*

- implementing other counter-measures that may reduce or eliminate damage caused by natural or man-made disasters;
- acquiring damaged homes or businesses in flood-prone areas, relocating the structures and returning the property to open space, wetlands or recreational uses; and
- building community shelters and tornado safe rooms to help protect people in their homes, public buildings and schools in hurricane- and tornado-prone areas.

ACHIEVING PREPAREDNESS

Individual Federal, State, local, and Tribal jurisdictions are responsible for implementing the preparedness cycle in advance of an incident, with input and support from the private sector and nongovernmental organizations. In order for successful incident management to occur, it is necessary that all persons involved have a clear understanding of their roles and responsibilities in the NIMS. This is essential not only for traditional responders, but also for those acting in a policy, coordination, or support role.

Policy Role: any individual who assists in the development, editing, reviewing, passing, signing and /or formalizing policies, procedures and/or plans relating to incident management and/or emergency prevention, preparedness, response, recovery, and mitigation programs and activities.

Coordination Role: any individual who manages resources (personnel, equipment, supplies and/or funding), or any other efforts toward incident management and emergency prevention, preparedness, response, recovery, and mitigation programs and activities, as well as in support of all actions taken to assist State, local, or Tribal entities.

Support Role: any individual who assists efforts for incident management and emergency prevention, preparedness, response, recovery, and mitigation programs and activities, as well as in support of all actions taken to assist State, local, or Tribal entities.

The NIMS provides the mechanisms for personnel and organizations to work collectively by offering the tools to ensure and enhance preparedness. Preparedness elements provide or establish processes for planning; mutual aid; training; exercises; personnel qualification and certification; and equipment certification.

HOMELAND SECURITY PRESIDENTIAL DECLARATION–7, CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITIZATION, AND PROTECTION

Homeland Security Presidential Declaration 7 (HSPD–7) directed DHS to establish a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Federal departments and agencies have been directed t o identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies are to work with State and local governments and the private sector to accomplish this objective. This effort includes completion and implementation of the National Infrastructure Protection Plan (NIPP). This effort also includes coordination and integration, as appropriate, with other Federal homeland security, emergency management, and preparedness activities including the National Response Plan (NRP), the NIMS, and applicable national preparedness goals.

RELATIONSHIP BETWEEN NIMS AND OTHER NATIONAL PREPAREDNESS EFFORTS

Homeland Security Presidential Directive 8 (HSPD-8), *National Preparedness*, issued December 17, 2003, directed Department Homeland Security (DHS) to lead a national initiative to develop a National Preparedness System – a common and unified approach to "strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters and other emergencies."

To achieve the mandates of HSPD-8, DHS has implemented a Capabilities-Based Planning approach to national preparedness. Capabilities-Based Planning is defined as planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that demands prioritization and choice. The September 11, 2001, terrorist attacks and more recently the 2004 and 2005 hurricane seasons illustrated the wide range of incidents that may occur across the Nation. Further, these events demonstrated that catastrophic incidents, whether man-made or naturally occurring, quickly exceed the capacity of any single jurisdiction. Capabilities-based planning defines the type, amount, and source of capabilities necessary at all levels of government across the country.

The requirements of HSPD-8 led to preparation of the Interim National Preparedness Goal which was developed to provide the means for the Nation to answer three fundamental questions:

- How prepared do we need to be?
- How prepared are we?
- How do we prioritize efforts to close the gap?

HSPD-8 also required DHS to develop mechanisms for the improved delivery of Federal preparedness assistance to State and local governments; and to strengthen the Nation's preparedness capabilities. Fifteen National Planning Scenarios were developed to illustrate the range, scope, magnitude, and complexity of events for which the Nation should prepare. Using this wide range of possible scenarios, including terrorism, natural disasters, and health emergencies, helps reduce uncertainty in planning and avoids focusing on any one threat, hazard, or set of conditions.

After identifying the most important performance needs across the scenarios, DHS then developed the Target Capabilities List (TCL) which is designed to guide efforts to build a national network of capabilities that will be available when and where they are needed to prevent, protect against, respond to, and recover from major events. Furthermore, the TCL defines the roles that all levels of government, NGOs, the private sector, and citizens have in national preparedness. The capabilities and associated target levels are identified in the TCL (listed in Table 2 below).

Table 2—The Target Capabilities List

Common Capabilities • Planning • Communications • Community Preparedness and Participation • Risk Management **Prevention Mission Capabilities** • Information Gathering and Recognition of Indicators and Warnings • Intelligence Analysis and Production • Information Sharing and Dissemination • Law Enforcement Investigation and Operations • CBRNE Detection **Protect Mission Capabilities** • Critical Infrastructure Protection • Food and Agriculture Safety and Defense • Epidemiological Surveillance and Investigation • Public Health Laboratory Testing **Response Mission Capabilities** • Onsite Incident Management • Emergency Operations Center Management • Critical Resource Logistics and Distribution • Volunteer Management and Donations • Responder Safety and Health • Public Safety and Security • Animal Health Emergency Support	**Response Mission Capabilities (continued)** • Environmental Health • Explosive Device Response Operations • Firefighting Operations/Support • WMD/Hazardous Materials Response and Decontamination • Citizen Evacuation and Shelter-in-Place • Isolation and Quarantine • Urban Search and Rescue • Emergency Public Information and Warning • Triage and Pre-Hospital Treatment • Medical Surge • Medical Supplies Management and Distribution • Mass Prophylaxis • Mass Care (Sheltering, Feeding and Related Services) • Fatality Management **Recovery Mission Capabilities** • Structural Damage and Mitigation Assessment • Restoration of Lifelines • Economic and Community Recovery

ORGANIZING FOR PREPAREDNESS

A jurisdiction has the responsibility to coordinate various preparedness activities among all appropriate agencies within the jurisdiction, as well as across jurisdictions. Additionally, private sector and NGOs must be involved in these efforts, since they are often used as the mode to deliver incident-related government services, and as they are the owners and operators of critical infrastructure and key resources that may be involved in incident management. Though not integrated directly into the NIMS, individual citizens play a critical role in preparedness and are expected to prepare themselves and their families for all types of potential incidents. Jurisdictions should have outreach programs to promote and support citizen preparedness (e.g. public education, training sessions, demonstrations, etc.).

PREPAREDNESS ORGANIZATIONS

Preparedness organizations provide interagency coordination for incident management activities before a potential incident. These organizations range from groups of individuals to small committees to large standing organizations which represent a wide variety of committees, planning groups, and other organizations (e.g. Citizen Corps, Local Emergency Planning Committees (LEPCs), Joint Terrorism Task Force (JTTF), Critical Infrastructure, etc.). Preparedness organizations should meet regularly and coordinate with one another to ensure an appropriate focus on helping jurisdictions and groups of jurisdictions to meet their preparedness needs. The needs of the jurisdictions involved will dictate how frequently such organizations must conduct their business, as well as how they are structured. When preparedness activities routinely need to be accomplished across jurisdictions, preparedness organizations should be multi-jurisdictional and/or multi-agency. Preparedness organizations at all jurisdictional levels should:

- establish and coordinate emergency plans and protocols including public communications and awareness;
- integrate and coordinate the activities of the jurisdictions and functions within their purview;
- establish the standards, guidelines, and protocols necessary to promote interoperability among member jurisdictions and agencies;
- adopt standards, guidelines, and protocols for providing resources to requesting organizations, including protocols for incident support organizations;
- set priorities for resources and other requirements;
- encourage and facilitate the ability of jurisdictions, their associated departments and agencies, and their residents to train, exercise and evaluate their preparedness regularly;
- ensure the establishment and maintenance of multi-agency coordination mechanisms, including Emergency Operations Centers (EOC), mutual-aid agreements, incident information systems, NGO and private sector outreach, public awareness and information systems, and mechanisms to deal with information and operations security;

- use multi-agency coordination mechanisms, as needed, for planned events (such as parades, sporting events, etc.) or for specific topics (such as pandemic influenza, hurricanes, etc.);[11] and
- plan for operational scientific support, which can be done at each level of government, and contribute ideas to ongoing research and development of new technologies.[12]

ROLE OF ELECTED AND APPOINTED OFFICIALS

For successful incident management, elected and appointed officials must have a clear understanding of their roles and responsibilities outlined in the NIMS. Elected and appointed officials include all administrative and political personnel who have leadership roles in a jurisdiction. At times, their roles may require providing direction and guidance to constituents during an emergency incident, but their day-to-day activities do not focus on emergency and incident management. Such officials may include elected legislators and chief executives, whether elected (e.g., governors and mayors) or appointed (e.g., county executives and city managers).

To better serve their constituents, particularly preparing for and during catastrophic events, elected and appointed officials should:

- understand, commit to, and receive training on the NIMS;
- maintain an understanding of basic emergency management and jurisdictional response capabilities;
- lead and motivate preparedness efforts within the community and agencies of the jurisdiction;
- help to establish appropriate relationships with other jurisdictions;
- support and encourage participation in mitigation and risk reduction efforts within the jurisdiction;
- provide guidance to their offices for the NIMS implementation with clearly stated policies; and
- understand laws and regulations in their jurisdiction that pertain to incident management.

Elected and appointed officials may also be called upon to help (re)shape law, policy, and budgets to aid preparedness efforts and to improve incident management.

Any incident can have a mix of political, economic, social, environmental, and cost implications with potentially serious long-term effects. More and more frequently, incidents require multi-agency and/or multi-jurisdictional response, during which elected and appointed officials must make difficult decisions under crisis conditions. Elected and appointed officials must be aware of how NIMS can work to ensure cooperative response efforts, thereby minimizing the potential implications of an incident.[13]

---

[11] See page 66. Component IV: Command and Management, *Multi-agency Coordination Systems.*

[12] See page 89. Ongoing Management and Maintenance, *Supporting Technologies.*

[13] ICS courses are available for Elected and Appointed Officials (e.g. G402, Incident Command System (ICS) *Overview for Executives/Senior Officials*).

ROLE OF NONGOVERNMENTAL ORGANIZATIONS

Nongovernmental organizations (NGO), such as community-based, faith-based, and national organizations including the American Red Cross, play vital roles in incident management at all levels. To fully integrate their efforts, NGOs should be included in a jurisdiction's preparedness efforts, especially planning, training and exercises. Furthermore, memoranda of understanding/memoranda of agreement should be established with NGOs prior to an incident so each organization will be aware of the capabilities, expectations, and roles of others.

It is recommended that key executives and administrators of NGOs use the NIMS for pre-planned events or incidents. The use of the NIMS improves the ability of the organizations to integrate into incident management. Compliance with the NIMS for internal management is not mandated but will support the continued integration of the NGOs into a jurisdiction's preparedness efforts.

ROLE OF PRIVATE SECTOR

The private sector plays a role in incident management and should be incorporated into all aspects of the NIMS. Utilities, industries, corporations, businesses, and professional and trade associations typically are involved in critical aspects of incident response. These organizations should prepare (e.g., planning, training and exercises) for all-hazard events that may affect their ability to deliver goods and services. It is essential that private sector organizations who are directly involved in emergency response and incident management (e.g. hospitals, utilities, and suppliers of critical resources) are included in all jurisdictions' preparedness efforts. Memoranda of understanding/memoranda of agreement should be established with these organizations prior to an incident so each party will be aware of the capabilities, expectations, and roles of the other. Finally, the private sector may be a source for best practices in many areas of preparedness and incident response.

INCORPORATION OF FEDERAL ASSETS

The Federal government has a pre-defined framework for Federal response to incidents requiring coordinated response, including Incidents of National Significance and other events that require Federal assets.[14] Jurisdictions should be aware of these Federal plans in order to accommodate Federal resources, if necessary.

NIMS AND THE NATIONAL RESPONSE PLAN

The NRP is an all-hazards plan built upon the NIMS framework that provides the structure and mechanisms to ensure timely and effective Federal support

[14] This response framework for Incidents of National Significance is specified in the NRP.

The NIMS provides the template for incident management regardless of size, scope, or cause of the event. The NRP is an all-hazards plan built upon the NIMS framework that provides the structure and mechanisms for national-level policy and operational direction for incident management to ensure timely and effective Federal support. The NRP is applicable to all Federal departments and agencies that have primary jurisdiction for or participate in operations requiring coordinated Federal response. The NRP identifies how Federal departments and agencies will respond to State, Tribal, and/or local requests for assistance.

The NRP and the NIMS are designed to improve the Nation's incident management capabilities and overall efficiency. During Incidents of National Significance or other incidents requiring significant Federal support, the NRP (based on the NIMS) works to integrate the capabilities and resources of various governmental jurisdictions, incident management and emergency response disciplines, nongovernmental organizations (NGOs), and the private sector into a cohesive, coordinated, and seamless national framework for incident management.

A basic premise of both the NIMS and the NRP is that incidents are generally handled at the lowest jurisdictional level possible. In the vast majority of incidents, local resources and local mutual aid will provide the first line of emergency response and incident management. When both local and State resources and capabilities are overwhelmed, Governors may request Federal assistance; however, the NIMS is designed so that local jurisdictional authorities retain command, control, and authority over response. Adhering to the NIMS will allow local agencies to better utilize incoming coordinated resources.

The NIMS and the NRP enable local jurisdictional authorities to retain command, control, and authority over response.

PREPAREDNESS ELEMENTS

Preparedness efforts should validate and maintain plans, policies, and procedures, describing how they will prioritize, coordinate, manage, and support personnel, information, equipment, and resources. The elements described below (preparedness planning, mutual-aid agreements, training and exercises, organizing personnel, using standardized qualifications and certification, and obtaining, preparing and maintaining equipment that meets set standards) build the foundation necessary for efficient and effective response. Ongoing support to preparedness organizations is provided by the NIC; in particular, the NIC supports: training and exercises, personnel qualification and certification, and equipment certification.[15]

[15] See page 81. Ongoing Management and Maintenance, *NIMS Integration Center.*

PREPAREDNESS PLANNING

Plans should incorporate accurate analyses of hazards and assessments of risks and vulnerabilities to ensure that capabilities required are available when and where they are needed. Plans should integrate all relevant departments, agencies, and jurisdictions (at all levels of government). Where appropriate, these plans should incorporate a mechanism for requesting assistance with clearly delineated processes for seeking and requesting assistance from necessary agency(s). While recognizing that jurisdictions and/or organizations will develop multiple types of plans, such as response, mitigation and recovery plans, it is essential that these plans are coordinated and complement one another.

Planning should focus on successful achievement of a plan's desirable outcomes. Plans must be realistic, scalable, and able to address all types of incidents, from daily occurrences to catastrophic events. Additionally, during large-scale incidents, planning organizations may be expected to contribute to operational planning. Plans should form the basis of training and be exercised periodically to ensure that all individuals involved in response are able to execute their assigned tasks. It is essential that plans address training and exercising, and allow for the incorporation of after action reviews and lessons learned following any major incidents or exercises.

Plans describe how personnel, equipment, and other governmental and non-governmental resources will be used to support incident management requirements. They represent the operational core of preparedness and provide mechanisms for setting priorities, integrating multiple entities and functions, establishing collaborative relationships, and ensuring that communications and other systems effectively support the full spectrum of incident management activities. Plans should also incorporate strategies for maintaining continuity of government and continuity of operations during and after incidents, as well as incorporate the advance planning associated with resource management and communications and information management.

Two categories of plans are defined as follows:

- **Strategic plans** develop programmatic priorities that address mission requirements, goals, objectives, milestones, and resources that ensure interoperable and integrated actions among all levels of government, the private sector and NGOs to manage all-hazard, incident-related prevention, protection, response, and recovery.
- **Operational plans** identify and direct the entities and resources required to execute the functional mission areas[16] based on the strategic planning. Operational plans often include (but are not limited to) contingency and tactical plans.

Jurisdictions should develop plans that define the scope of preparedness and incident management activities necessary for that jurisdiction.[17] (An example of this type of plan is an Emergency Operations

[16] Preparedness, prevention, protection, response, and recovery

[17] State and Local Guide (SLG) 101: Guide for All-Hazard Emergency Operations Planning, provides emergency managers and other emergency services personnel with information on developing risk-based, all-hazard emergency operations plans.

Plan.) These plans should describe organizational structures, roles and responsibilities, policies, and protocols for providing emergency support and should be flexible enough for use in all emergencies. While the preparedness of the public is generally beyond the scope of the NIMS, plans should also include pre-incident and post-incident public awareness, education, and communications plans and protocols.

PROCEDURES AND PROTOCOLS

Each entity involved in incident management should develop procedures and protocols that translate into specific action-oriented checklists, including how the organization will accomplish its assigned tasks, for use during incident management operations. Oftentimes procedures and protocols are the specific actions one can take to implement the plan. Procedures are documented and implemented with checklists; resource listings; maps, charts, and other pertinent data; mechanisms for notifying staff; processes for obtaining and using equipment, supplies, and vehicles; methods of obtaining mutual aid; mechanisms for reporting information to organizational work centers and EOCs; and communications operating instructions, including connectivity with private sector and nongovernmental organizations. The development of procedures is required in accordance with the law for certain risk-based, hazard-specific programs. There are four standard levels of procedural documents:

- Overview—a brief concept summary of an incident-related function, team, or capability;
- Standard Operating Procedure (SOP) or Operations Manual—a complete reference document that details the procedures for performing a single function or a number of interdependent functions;
- Field Operations Guide (FOG) or Handbook—a durable pocket or desk guide that contains essential information required to perform specific assignments or functions; and
- Job Aid—a checklist or other aid that is useful in performing or training for a job.

MUTUAL-AID AGREEMENTS

Mutual-aid agreements are the means for one entity to provide resources, facilities, services, and other required support to another entity during an incident. There are several types of mutual aid including:

- Automatic Mutual Aid: Units for neighboring jurisdictions are automatically dispatched to the scene as part of automatic mutual-aid agreements. These inter-local agreements are usually basic contracts; some may be informal accords.
- Local Mutual Aid: Agreements are between neighboring jurisdictions and involve a formal request for assistance. Mutual aid is activated less often than automatic mutual aid but covers a larger geographic area.
- Regional Mutual Aid: Units that are part of a regional mutual-aid agreement can assist local units that have been on-scene for an extended period. Regional mutual-aid agreements exist between multiple jurisdictions and are often sponsored by a council of governments or a similar regional body.

- Statewide/Intrastate Mutual Aid: Increases the number of on-scene units. These agreements, often coordinated through the State, incorporate both State assets and local assets in an attempt to increase preparedness statewide.

- Inter-state Agreements: Out-of-state assistance through Emergency Management Assistance Compact (EMAC) or other formal state-to-state agreements that support the response effort and onward into the recovery phase.[18]

- Other Mutual Aid: Any agreement, whether formal or informal, used to request and/or provide assistance and/or resources between jurisdictions at any level of government.

Mutual-aid agreements should include the following elements or provisions:

- definitions of key terms used in the agreement;
- roles and responsibilities of individual parties;
- procedures for requesting and providing assistance;
- procedures, authorities, and rules for payment, reimbursement, and allocation of costs;
- notification procedures;
- protocols for interoperable communications;
- relationships with other agreements among jurisdictions;
- workers compensation;
- treatment of liability and immunity;
- recognition of qualifications and certifications; and
- sharing agreements, as required.

Each jurisdiction should be party to mutual-aid agreements with the appropriate jurisdictions from which they expect to receive or to which they expect to provide assistance during an incident. This would normally include all neighboring or nearby jurisdictions, as well as relevant private sector and nongovernmental organizations. States should participate in inter-state compacts and look to establish intrastate agreements that encompass all local jurisdictions. Agreements, such as Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA), are also needed with the private sector, nongovernmental organizations, such as community-based, faith-based, and national organizations including the American Red Cross, to facilitate the timely delivery of private assistance at the appropriate jurisdictional level during incidents.

Authorized officials from each of the participating jurisdictions will collectively approve all mutual-aid agreements.

TRAINING AND EXERCISES

Personnel with roles in incident management at all levels of government—including persons with leadership positions, such as elected and appointed officials—and within the private sector and

[18] "Mutual-aid: Multi-jurisdictional Partnerships for Meeting Regional Threats" U.S Department of Justice Office of Justice Programs Bureau of Justice Assistance NCJ210679 September 2005.

nongovernmental organizations, must be appropriately trained to improve all-hazards incident management capabilities nationwide. Personnel with roles in incident management must also participate in realistic exercises—including multi-disciplinary and multi-jurisdictional events and private sector and nongovernmental organization (NGO) interaction—to improve integration and interoperability. Training involving standard courses on incident command and management, incident management structure, operational coordination processes and systems—together with courses focused on discipline-specific and agency-specific subject-matter expertise—helps to ensure that personnel at all jurisdictional levels and across disciplines can function effectively together during an incident.[19] Training and exercises should be specifically tailored to the responsibilities of the personnel involved in incident management. Mentoring or shadowing opportunities should not be overlooked and should be incorporated to enhance training and exercising.

TRAINING

NIMS training levels should be dependent upon the individual's/jurisdiction's level of involvement in incident management activities. Training should allow:

- agencies to use the concepts and principles of the NIMS in all incidents; and
- practitioners to become more comfortable using the NIMS, including the incident command system.

EXERCISES

Exercises should be designed to test the NIMS implementation thoroughly. Thorough exercising of the NIMS elements and subsystems may be done using a single comprehensive exercise or a series of exercises, each of which tests specific aspects of the NIMS and its subsystems. Exercises should be conducted with parties to the jurisdiction's Emergency Operations Plan (EOP) including local departments and agencies, mutual aid partners, etc. More specifically, exercises should cover:

- all aspects of a plan, particularly the processes/procedures of activating local, intrastate, or interstate mutual-aid agreements; and
- administrative knowledge needed to activate those agreements.

PERSONNEL QUALIFICATIONS AND CERTIFICATION

Under the NIMS, preparedness is based on national standards and common organization for the qualification and certification of emergency response personnel. Standards will help ensure that participating agencies' and organizations' field personnel possess the minimum knowledge, skills, and experience necessary to execute incident management and emergency response activities safely and effectively. Standards typically include training, experience, credentialing, currency, and physical and medical fitness. Personnel who are certified for employment in support of an incident that transcends a

[19] The NIC supports training and exercise development. See page 81. Ongoing Management and Maintenance, *NIMS Integration Center*.

States' jurisdictions through the EMAC System will be required to meet national qualification and certification standards. Federal, State, local, and Tribal certifying agencies; professional organizations; and private organizations should credential personnel for their respective disciplines and/or jurisdictions.[20] Organizing personnel into "typed" teams of resources ensures the ability to scale the response to an incident quickly and in a flexible manner to obtain requested assistance.

EQUIPMENT CERTIFICATION

Incident management and emergency responder organizations at all levels rely on various types of equipment to perform mission essential tasks. A critical component of operational preparedness is the acquisition of equipment that will perform to certain standards, including the capability to be interoperable with equipment used by other jurisdictions.[21] Associated with this is the need to have a common understanding of the abilities of distinct types of equipment, to allow for rapid scaling and flexibility in meeting the needs of an incident.

[20] The NIC manages specification of personnel qualification and certification. See page 81. Ongoing Management and Maintenance, *NIMS Integration Center*.

[21] The NIC manages specification of equipment certification. See page 81. Ongoing Management and Maintenance, *NIMS Integration Center*.

COMPONENT II

COMMUNICATIONS AND INFORMATION MANAGEMENT

Effective incident management relies upon flexible and scalable communications and information systems that provide a common operating picture to all command and coordination sites. These systems provide effective communications in the field and among command and coordination sites, share incident management data between support, command and coordination sites, and ensure adequate sharing of information and intelligence pertinent to the incident. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are principal goals of communications and information management. A common operating picture and interoperability provide the framework necessary to:

- formulate and disseminate information including indications and warnings, instructions, etc.;
- formulate, execute, and communicate operational decisions at an incident site, as well as between incident management entities across jurisdictions and functional agencies;
- prepare for potential requirements and requests supporting incident management activities; and
- develop and maintain overall awareness and understanding of an incident within and across jurisdictions.

Prior to an incident, entities responsible for taking appropriate pre-incident actions use communications and information management processes and systems to inform and guide various critical activities. These actions include mobilization or pre-deployment of resources, as well as strategic planning by preparedness organizations, multi-agency coordination entities[22], agency executives, jurisdictional authorities, and EOC personnel. During an incident, incident management personnel use communications and information processes and systems to inform the formulation, coordination, and execution of operational decisions and requests for assistance.

[22] For the purpose of this document multi-agency coordination entities and multi-agency coordination groups are interchangeable terms.

CONCEPTS AND PRINCIPLES

COMMON OPERATING PICTURE

A common operating picture provides a broad overview of the overall situation allowing incident managers at all levels to make effective, consistent, and timely decisions. Integrated systems for communication, information management, and intelligence and information sharing allow data to be continuously updated during an incident, providing a common framework that covers the incident's life-cycle across jurisdictions and disciplines. A common operating picture helps ensure consistency at all levels of incident management across jurisdictions, as well as between various governmental jurisdictions and private sector and nongovernmental entities that are engaged.

Interoperability. The emergency communications system should be the same or linked to the same system that the jurisdiction uses for non-emergency procedures, and should effectively interface with national standards as they are developed. The system should allow the sharing of data with other jurisdictions and levels of government during planning and deployment.

[IS-703 course]

COMMON COMMUNICATIONS AND DATA STANDARDS

Common communications and data standards and related testing and compliance mechanisms are fundamental to an effective NIMS. Communications interoperability in the context of incident management is also critical. Effective communications outside the incident structure—between other levels of government and between government and private entities—for resources and other support is also enhanced by adherence to such standards. Progress toward common communications and data standards and systems interoperability will be accomplished over time through a sustained collaborative effort facilitated by the NIMS Integration Center (NIC).

MANAGING COMMUNICATIONS AND INFORMATION

The NIMS communications and information systems enable the essential functions needed to provide a common operating picture and interoperability for incident management at all levels in two ways, (1) incident management communications and (2) information management.

INCIDENT MANAGEMENT COMMUNICATIONS

Entities must ensure that communications capabilities are sufficiently diverse and reliable. Effective communications processes and systems must exist to support the complete spectrum of incident management activities. The following two principles apply:

INDIVIDUAL JURISDICTIONS

Jurisdictions will be required to comply with national interoperable communications standards, once developed. Standards appropriate for NIMS users will be designated by the NIC in partnership with recognized standards development organizations (SDOs).

INCIDENT COMMUNICATIONS

These will follow the characteristics called for under the ICS. Communications at an incident is best managed using a common communications plan. Often times during complex incidents (with multiple operational periods) an incident- based communications center may be established solely for use by the command, tactical, and support resources assigned to the incident. All entities involved in incident management will utilize common terminology for communications.

INFORMATION MANAGEMENT

The NIC is charged with the coordination and maintenance of the information framework required to guide the development of NIMS-related information systems. This framework consists of documented policies and interoperability standards.

POLICIES

PRE-INCIDENT INFORMATION

Pre-incident information needs are met at the Federal, State, local, and Tribal levels, in concert with the private sector and NGOs, primarily through the preparedness organizations.[23]

INFORMATION MANAGEMENT

The information management system provides guidance, standards, and tools to enable Federal, State, local, Tribal, and private sector and nongovernmental entities to integrate their information needs into a common operating picture.

NETWORKS

Indications and warnings, incident notifications and public communications, and the critical information that constitute a common operating picture are disseminated through a combination of networks used by EOCs. Notifications are made to the appropriate jurisdictional levels and to private sector and nongovernmental organizations through the mechanisms defined in emergency operations and incident action plans at all levels of government.

TECHNOLOGY USE

Agencies must plan in advance for the effective and efficient use of information management technologies (e.g., computers and networks) to tie together all command, tactical, and support units involved in incident management and to enable these entities to share information critical to mission execution and the cataloguing of required corrective actions.

INTEROPERABILITY STANDARDS

Facilitating the development of data standards for the functions described below, including secure communications when required, is the responsibility of the NIC.[24] Standards will be developed in accordance with the following design goals.

INCIDENT NOTIFICATION AND SITUATION REPORT

Incident notification takes place at all levels. Although notification and situation report data must be standardized, it must not prevent information unique to a reporting organization from being collected or disseminated. Standardized transmission of data in a common format enables the passing of appropriate notification information to a national system that can handle data queries and information and intelligence assessments and analysis.

---

[23] See page 11. Component I: Preparedness, *Preparedness Organizations*.

[24] See page 81. Ongoing Management and Maintenance, *NIMS Integration Center*.

STATUS REPORTING

All levels of government initiate status reports (e.g., Situation Reports and Pollution Reports) and then disseminate them to other jurisdictions. A standardized set of data elements will be defined to facilitate this process.

ANALYTICAL DATA

Analytical data, such as information on public health and environmental monitoring, are collected in the field in a manner that observes standard data definitions. It is then transmitted to laboratories using standardized analysis processes. During incidents that require public health and environmental sampling, multiple organizations at different levels of government often respond and collect data. Standardization of sampling and data collection enables more reliable laboratory analysis and improves the quality of assessments provided to decision-makers.

GEOSPATIAL INFORMATION

Geospatial information is used to integrate assessments, situation reports, and incident notification into a coherent common operating picture and as a data fusion and analysis tool to synthesize many kinds and sources of data and imagery. Correct utilization of geospatial data is increasingly important to decision-makers. Processes for managing geospatial intelligence capabilities must be managed through preparedness efforts and integrated within command, coordination, resource management, and public information systems. The use of geospatial data must be tied to consistent standards because of the potential for coordinates to be transformed incorrectly or otherwise misapplied, causing inconspicuous, yet serious errors. Standards covering geospatial information should also be robust enough to enable systems to be used in remote field locations or devastated areas where telecommunications capabilities may not have sufficient bandwidth to handle large images or are limited in terms of computing hardware.

WIRELESS COMMUNICATIONS

To ensure that incident management organizations can communicate and share information with each other through wireless systems, the NIMS will include standards to help ensure that wireless communications and computing for Federal, State, local, and Tribal public safety organizations, private sector and NGOs are interoperable.

IDENTIFICATION AND AUTHENTICATION

Individuals and organizations who access the NIMS information management system and, in particular, those who contribute information to the system (e.g., situation reports), must be properly authenticated and certified for security purposes. This requires a national-authentication and security-certification standard that is flexible and robust enough to ensure that information can be properly authenticated and protected. While the NIC is responsible for facilitating development of these standards, different levels of government and private organizations must collaborate to administer the authentication process.

NATIONAL DATABASE OF INCIDENT REPORTS

Through the NIC, Federal, State, local, and Tribal organizations responsible for receiving initial incident reports will work collaboratively to develop and adopt a national database of incident reports that can be used to support incident management efforts.

COMPONENT III

RESOURCE MANAGEMENT

Incident management requires carefully managed resources to meet critical incident needs. Utilization of the standardized resource management principles of the NIMS such as typing, inventorying, and tracking, will facilitate the dispatch, deployment, and recovery of resources during and after an incident. Resource management must be flexible and scalable in order to support any incident and be adaptable to real-time changes in incident size and scope. Efficient, effective deployment of resources requires that resource management spans the life-cycle of an incident, from preparedness to response to recovery.

From small, single-agency incidents up through Incidents of National Significance, resource management involves coordinating and overseeing the application of tools, processes, and systems that provide incident managers with timely and appropriate resources during an incident. As incident response grows in size, or when an incident starts as a large-scale event, local incident managers may require resources from other local jurisdictions; other levels of government (possibly including military support), the private sector; and/or nongovernmental organizations. Incident resources may include personnel, teams, facilities, equipment, and funding streams. Resources may support field and command operations through the incident command post (ICP), or function within the multi-agency coordination systems, serving at an emergency operations center or similar site. Resource management systems must be able to adapt to any incident whatever its geographic scale and disciplinary complexity.

Resource management systems must support adequate communication between the command and coordination functions to manage resources effectively. Incident Command sets incident priorities and makes resource requests. Resource management systems, both manual and automated, then process the resource request. The resources requested are either filled locally or through agreements (e.g. EMAC). In a case of competition for critical resources, Multi-Agency Coordination entities prioritize and coordinate resource allocation and distribution, according to resource availability, needs of other incidents, and other constraints and considerations. This process follows established rules developed using the Multi-Agency Coordination System.

Operationally, resource management involves four primary tasks:

TRAINING & EXERCISING

A key element of preparedness is training and exercising resource management systems.

Resource managers—both EOC and incident managers—should be trained to know:

- the resources available
- how to obtain them
- how to deliver/receive resources
- systems to track resources

[FEMA/EMI IS-703 course]

- establishing systems for describing, inventorying, requesting, and tracking resources;
- activating these systems prior to and during an incident;
- dispatching resources prior to and during an incident; and
- demobilizing or recalling resources during or after incidents.

To ensure resources and resource management systems are ready to respond to an incident, it is essential that preparedness efforts include training and exercising the systems used for requesting, tracking, and receiving resources.

Operational resource management is supported by the implementation of resource management systems or processes as part of the NIMS that allow resource management to be conducted more efficiently and effectively. The standardized procedures, methodologies, and functions that comprise these resource management systems ensure that resources deploy quickly and efficiently to support incident management.

CONCEPTS AND PRINCIPLES

CONCEPTS

The underlying concepts of resource management are:

- provision of a uniform method of identifying, acquiring, allocating, and tracking resources;
- use of effective mutual aid and donor assistance and is enabled by the standardized classification of kinds and types of resources required to support the incident management organization;
- use of a credentialing system tied to uniform training and certification standards to ensure that requested personnel resources are successfully integrated into ongoing incident operations;
- coordination as a responsibility of an emergency operations center (EOC), as well as specific elements of the ICS structure (e.g., the Resources Unit within the Planning Section);
- inclusion of resources contributed by the private sector and NGOs; including those resources mobilized for restoration of publicly or privately owned critical infrastructure or key resources; and
- appropriate intelligence analysis tools and mechanisms designed to support sound resource management decision-making processes.

PRINCIPLES

The foundations of resource management are five interwoven principles that follow the life-cycle of an incident: (1) Planning, (2) Use of Agreements, (3) Categorizing Resources, and (4) Resource Identification and Ordering, and (5) Effective Management of Resources.

PLANNING

Preparedness organizations work together in advance of an incident to develop plans for managing and employing resources.[25] Coordinated planning, training to common standards, and multi-agency exercises provide a foundation for interoperability and compatibility of resources throughout an incident. Planning should continually and accurately assess the current preparedness environment and readiness of resources for an entity or jurisdiction.

PRE-DEPLOYMENT STRATEGIES

For certain kinds of incidents, resource needs may be anticipated well enough to develop pre-planned deployment strategy, incorporating all elements of resource management.

- **Pre-incident assignment:** Assigning personnel and teams to specific tasks in anticipation of incident response.
- **"Move-up" or "backfill" strategy:** Moving resources nearest to an incident into the incident area, with more distant resources filling the void by backfilling behind the deploying resources.
- **Regional pre-deployment staging:** Using pre-designated staging areas for final preparation of resources prior to mobilization and recovery of resources during demobilization.

Planning may include the creation of new policies to encourage pre-positioned resources. Pre-positioned resources are resources moved to an area near the expected incident site, based on a resource need that is anticipated by an EOC or other resource coordination unit; such resources contrast with assigned resources. Plans should anticipate and specify incident triggers—thresholds that escalate the response, such as introduction of Federal resources, or that demand a specific reaction, such as the restocking of certain supplies when inventory reaches a certain point. Organizations should be familiar with Federal agency responses to catastrophic incidents, such as major hurricanes, and should be prepared to utilize (e.g. US&R Task Force) and/or coordinate with (e.g. Individual Assistance) Federal assets, including possible pre-incident deployment of Federal assets.[26]

USE OF AGREEMENTS

Pre-incident agreements among all parties providing or requesting resources are necessary to enable effective and efficient resource management during incident operations. This would include agreements and pre-incident contracts for service and/or supplies that may need to be secured during an incident.

---

[25] See page 11. Component I: Preparedness, *Preparedness Organizations.*

[26] The specific response framework for Incidents of National Significance is specified in the National Response Plan (NRP).

Formal pre-incident agreements (e.g., mutual aid and EMAC) between parties, both governmental and non-governmental, that might provide or request resources are established to ensure the employment of standardized, interoperable equipment, and other incident resources during incident operations.

CATEGORIZING RESOURCES

Resources may be organized by size, capacity, capability, skill, and other characteristics. This makes the resource ordering and dispatch process within and across jurisdictions, and among governmental and non-governmental entities more efficient and ensures that appropriate resources are received.

RESOURCE IDENTIFICATION AND ORDERING

Resource managers use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities. Resource managers perform these tasks either at Incident Command's request or in accordance with planning requirements.

Identification and ordering of resources are intertwined. In some cases, the identification and ordering process is compressed, where Incident Command may know the resources necessary for the task and specify a resource order directly. In larger, more complex incidents, Incident Command may not be aware of available resources to meet the incident demand, or an Area Command may need resources to meet a larger-scale collection of incident tasks. In this case, Incident Command will identify the operational need and work with resource managers in the multi-agency coordination system to identify and order resources.

STOCKPILING VS. JUST IN TIME

Resources may be acquired in advance and stored in a warehouse, i.e., "stockpiled," or supplied "just in time," typically using a pre-incident contract. Planning and resource accounting procedures should accommodate both types of resource supply.

CHOOSING A RESOURCE MANAGEMENT SYSTEM

There are many resource management systems on the market today; with various strengths and weaknesses. Key considerations when purchasing such systems include:

Ease of deployment. If the system is rarely used, it must be extremely simple.

Interoperability. Ideally, the emergency system should be the same or linked to the same system that the jurisdiction uses for non-emergency procedures, and should effectively interface with national standards, as they are developed.

[FEMA/EMI IS-703 course]

EFFECTIVE MANAGEMENT OF RESOURCES

Resource managers use validated practices to perform key resource management tasks systematically and efficiently. Examples include the following:

ACQUISITION PROCEDURES

These procedures are used to obtain resources to support operational requirements. Preparedness organizations develop tools and related standardized

processes to support acquisition activities. Examples include mission tasking, contracting, drawing from existing stocks, and making small purchases. Material resources may be acquired in advance and stockpiled or purchased "just in time" through appropriate pre-incident contract vehicles. A key part of acquisition procedures is developing methods and protocols for the handling and distribution of donated resources.

MANAGEMENT INFORMATION SYSTEMS

These systems are used to collect, update, and process data; track resources; and display their readiness status. They enhance information flow and provide real-time data in a fast-paced environment where different jurisdictions and functional agencies managing different aspects of the incident life-cycle must coordinate their efforts. Examples include geographical information systems (GISs), resource tracking systems, transportation tracking systems, inventory management systems, and reporting systems.

Management information systems should be based on common standards that incorporate resource accounting in anticipation of reimbursement requirements. Recovery of resource costs may require significant documentation and an audit of resource-related expenses incurred before and during an incident. Subsystems to manage resource ordering and demobilization should include accounting information sufficient to meet demands of reimbursing agencies, such as the Federal government.

REDUNDANT INFORMATION SYSTEMS

Management information systems should have sufficiently redundant and diverse power supplies and communication capabilities. Resource managers should also identify alternate backup systems to manage resources, in the event that the primary resource management system is disrupted or unavailable.

ORDERING, MOBILIZATION, DISPATCHING, AND DEMOBILIZATION PROTOCOLS

Protocols are used to request resources, prioritize requests, activate and dispatch resources to incidents, and return resources to normal status. Preparedness organizations develop standard protocols for use within their jurisdictions. Examples include tracking systems that identify the location and status of mobilized or dispatched resources and procedures to "demobilize" resources and return them to their original locations and status.

MANAGING RESOURCES

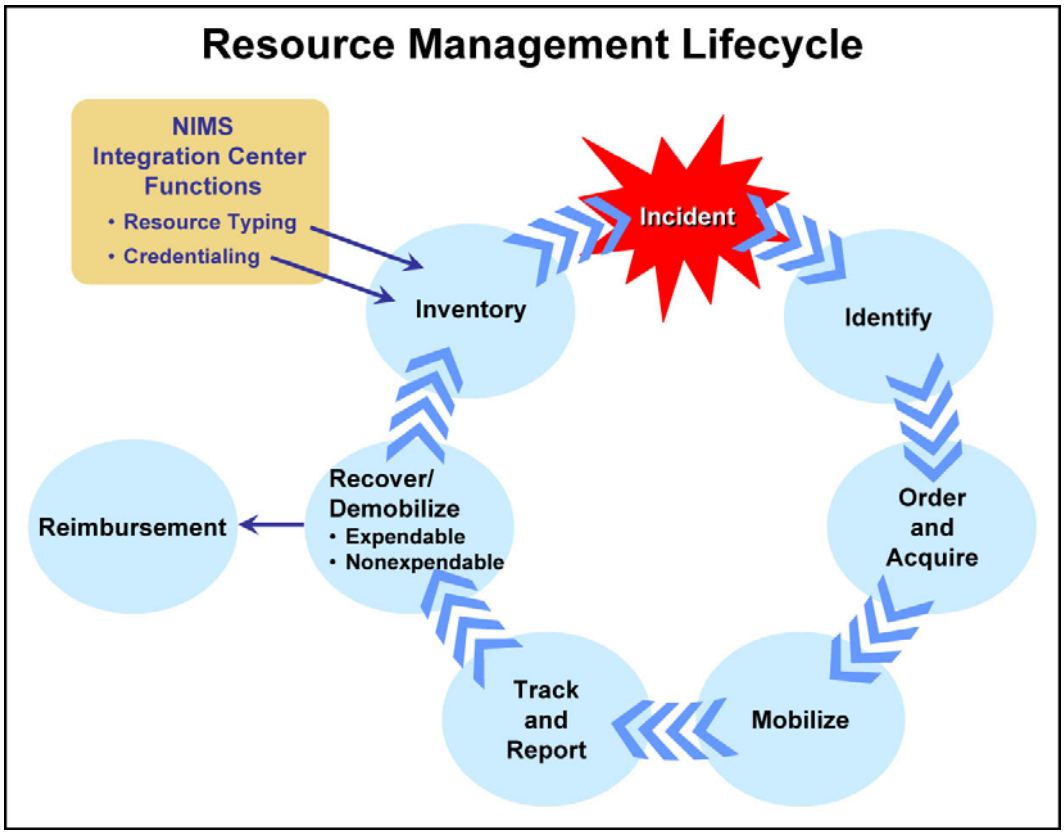


Figure 1—Resource Management Life-cycle

To implement these concepts and principles in performing the primary tasks of resource management, the NIMS includes standardized procedures, methodologies, and functions in its resource management processes. These processes reflect functional considerations, geographic factors, and validated practices within and across disciplines and are continually adjusted as new lessons are learned. The basic foundation for resource management provided in this component will be expanded and refined over time in a collaborative cross-jurisdictional, cross-disciplinary effort led by the NIC, discussed in the Ongoing Management and Maintenance component.[27]

The NIMS uses nine processes for managing resources; (1) identify and type resources, (2) certify, qualify, credential and badge personnel, (3) inventory resources, (4) identify resource requirements, (5)

[27] See page 81. Ongoing Management and Maintenance, *NIMS Integration Center*.

order and acquire resources, (6) mobilize resources, (7) track and report resources, (8) recover resources, and (9) reimbursement.

IDENTIFY AND TYPE RESOURCES

Resource typing entails categorizing by capability the resources that incident managers commonly request, deploy, and employ. Measurable standards identifying the capabilities and performance levels of resources serve as the basis for categories. Resource users at all levels identify these standards and then type resources on a consensus basis. Resource kinds may be divided into subcategories (types) to define more precisely the resource capabilities needed to meet specific requirements. Resource typing is a continuous process designed to be as simple as possible to facilitate frequent use and accuracy in obtaining needed resources.[28] To allow resources to be deployed and used on a national basis, the NIC, defined in the Ongoing Management and Maintenance component, is responsible for defining national resource typing standards.

RESOURCE TYPING
In the national resource typing protocol, resources are organized by:
Category: A category is the function for which a resource would be most useful, for example, public works and engineering or firefighting.
Kind: Kind refers to broad classes that characterize like resources, such as teams, personnel, equipment, vehicles, and aircraft.
Components: A resource may be comprised of several components. For example, the components of an urban search and rescue (US&R) task force include search team, medical team, heavy rescue team, logistics and management.
Metrics: Metrics are measurable standards which are useful in describing a resource's capability.
Type: Type refers to the level of resource capability. Assigning the Type 1 label to a resource implies that it has a greater level of capability based on its metrics than a Type 2 of the same kind of resource.
[FEMA/EMI IS-703 course]

The NIC ensures that the typing of resources reflects operational demands. While resource-typing documents define the makeup of typed equipment, personnel, and teams, the resource-typing system should also provide a demand or task-driven profile of resource orders according to typical operational needs.

CERTIFY, QUALIFY, CREDENTIAL AND BADGE PERSONNEL

Personnel certification and qualification entails authoritatively attesting that individuals meet professional standards for the training, experience, and performance required for incident-management functions. Credentials, based on certification and qualification, provide a system for resource managers and Incident Command to identify qualified personnel. Credentialing involves providing documentation that can authenticate and verify the certification and identity of designated incident managers and emergency responders. This system helps ensure that personnel representing various jurisdictional

[28] See Appendix A for a more complete discussion of the NIMS national resource typing protocol.

levels and functional disciplines possess a minimum common level of training, currency, experience, physical and medical fitness, and capability for the incident management or emergency responder position they are tasked to fill. Credentialing follows certification and qualification in the process of confirming that an emergency responder is capable of performing assigned critical tasks and capabilities. Figure 2 illustrates the stages involved in credentialing emergency responders.

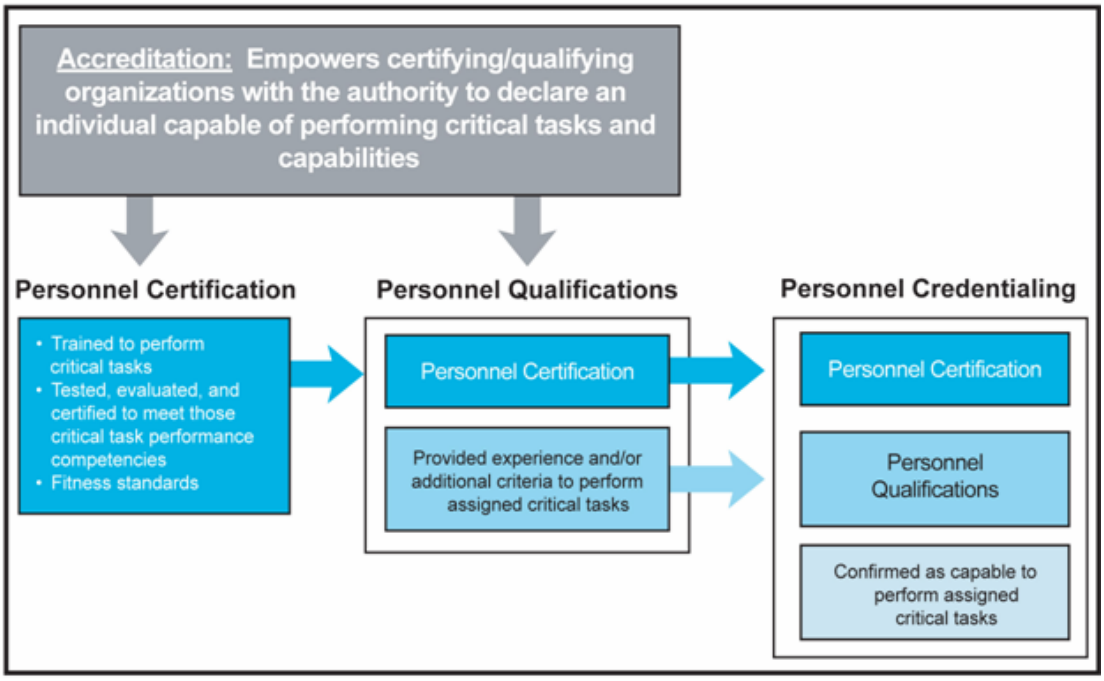


Figure 2—Process of Credentialing Emergency Responders[29]

INVENTORY RESOURCES

Resource managers use various resource inventory systems to assess the availability of assets provided by public, private, and volunteer organizations. Preparedness organizations enter all resources into resource tracking systems maintained at local, Tribal, State, regional, and national levels. The data are then made available to 911 centers, EOCs, and multi-agency coordination entities. The fact that resources are inventoried within an inventory system is not an indication of automatic availability. The local jurisdiction and/or owner of the resources has the final determination on availability.

A key aspect of the inventorying process is determining whether or not the primary-use entity needs to warehouse items prior to an incident. Resource managers make this decision by considering the urgency

[29] Figure identified as 007aFEMA, from the NIC credentialing working group, "Working Group Guidelines," v. 1.7 (April 2006).

of the need, whether there are sufficient quantities of required items on hand, and/or whether they can be produced quickly enough to meet demand. Another important part of the process is managing inventories with shelf-life or special maintenance considerations. Resource managers must build sufficient funding into their budgets for periodic replenishments, preventive maintenance, and capital improvements.

Deployable resources have different inventory, ordering, and response profiles, depending on their primary use during the response or recovery phases of an incident. Planning for use, inventory, and tracking of resources should recognize the fundamental difference in resource deployment in the response and recovery phases. The response phase relies heavily on mutual aid, with these resources generally leaving once response transitions to recovery. Recovery resources are typically acquired through contracts with the private sector. Systems for resource inventory, ordering, and tracking must be adaptable to all resource deployment profiles.

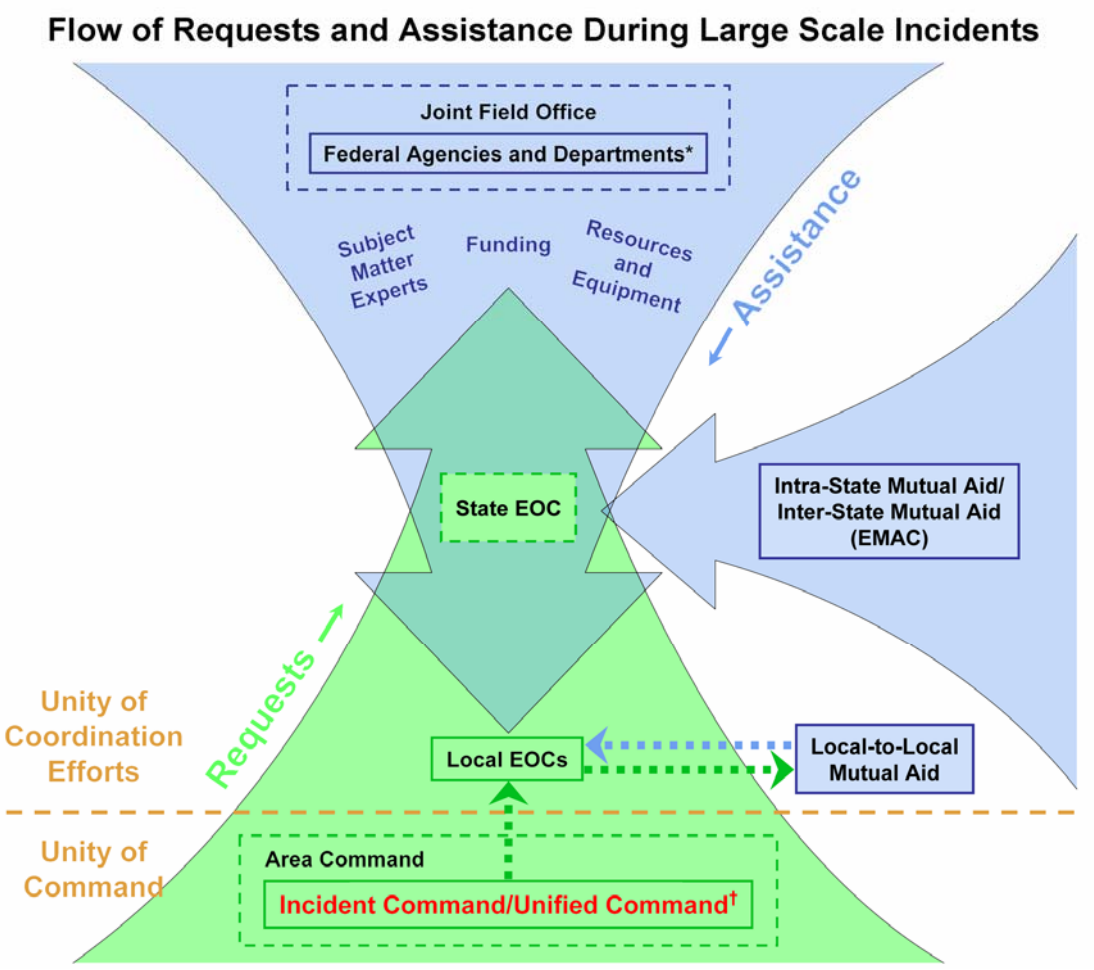
Inventory systems must account for the potential of double-counting personnel. In particular, resource summaries should clearly reflect any overlap of personnel across different resource pools. Personnel inventories should reflect single resources with multiple skills, taking care not to overstate the total resources. For example, many firefighters also have credentials as emergency medical technicians (EMT). A resource summary, then, could only count a firefighter as a firefighter or an EMT, but not as both. The total should reflect the number of available personnel, not simply the sum of the firefighter and EMT counts.

IDENTIFY RESOURCE REQUIREMENTS

Resource managers identify, refine, and validate resource requirements throughout the incident. This process involves accurately identifying (1) what and how much is needed, (2) where and when it is needed, and (3) who will be receiving or using it. Resources to be identified in this way include equipment, facilities, and incident management personnel and/or emergency response teams. If a requestor is unable to describe an item by resource type or classification system, resource managers provide technical advice to enable the requirements to be defined and translated into a specification. Specific resources for critical infrastructure work may need to be identified and coordinated through mutual aid systems unique to those critical infrastructure/key resources sectors, and should be accessible to the NIMS through preparedness organizations and multi-agency coordination systems.

Resource availability and requirements will constantly change as the incident evolves. Consequently, all entities participating in an operation must coordinate closely in this process. Coordination should begin as early in the preparedness phase as possible, ramping up at the earliest possible point in incident response.

There will be instances in which a potential incident is projected to have catastrophic implications (e.g., major hurricane), and States or the Federal government may activate a proactive response by pre-deploying assets to the potential incident area. In cases where there is time to assess the requirements and plan for a catastrophic incident, the Federal response and pre-positioning of Federal assets will be tailored to address the specific situation.



*Some Federal agencies (U.S. Coast Guard, EPA, etc.) have statutory responsibility for response and will coordinate directly with affected jurisdictions.

†Command function

Figure 3—Example Direction of Requests for Assistance

ORDER AND ACQUIRE RESOURCES

Requests for resources that Incident Command cannot obtain locally are submitted through a multi-agency coordinating entity, such as an EOC, using standardized resource-ordering procedures. If the multi-agency coordinating entity is unable to fill the order locally, the order is forwarded to the next

level—generally an adjacent locality, State, regional EOC, or another multi-agency coordination entity.[30]

AVOID BYPASSING SYSTEMS
All resource managers, including political leaders, should recognize the inherent limitation in requesting resources by reaching around the official resource coordination units within the multi-agency coordination system supporting the incident(s). These requests do not proceed within the context of orderly resource management systems and typically lead to inefficient use and/or lack of accounting of resources.

The decision cycles for placing and filling resource orders are different for field/incident resource managers and resource coordination units. Incident Command will develop resource requests for urgent needs and as defined for successive operational periods. Decisions about resources by coordination entities are set by agency protocol and possibly the resource demands of other incidents. Inventoried resources will only be mobilized with the consent of the jurisdiction that is being to provide the requested resources. Systems to order resources should be flexible enough to accommodate this difference. As one way to overcome delays in ordering and transportation of resources, resource coordinators may consider pre-positioning resources so that they are more readily available to Incident Command.

MOBILIZING RESOURCES

Incident personnel begin mobilizing when notified through established channels. At the time of notification, they are given the date, time, and place of departure; mode of transportation to the incident; estimated date and time of arrival; reporting location (address, contact name, and phone number); anticipated incident assignment; anticipated duration of deployment; resource order number; incident number; and applicable cost and funding codes. The resource tracking and mobilization processes are directly linked. When resources arrive on scene, they must formally check in. This starts the on-scene in-processing and validates the order requirements. Notification that the resource has arrived is sent back through the system.

For resource managers, the mobilization process may include planning for deployment,[31] equipping, training, designating assembly points that have facilities suitable for logistical support; and obtaining transportation to deliver resources to the incident most quickly, in line with priorities and budgets. Mobilization plans should also recognize that some resources are fixed facilities, such as laboratories, hospitals, EOCs, shelters, and waste management systems. These facilities ramp up operations on site without moving into the incident area in the way that other resources are mobilized. Plans and systems to monitor the status of resource mobilization should be flexible enough to adapt to both styles of mobilization.

---

[30] For the purpose of this document multi-agency coordination entity and multi-agency coordination group are interchangeable terms.

[31] Inter-agency mobilization guidelines at the Federal, regional, State, local, and Tribal levels provide direction for mobilization of resources.

Managers should plan and prepare for the demobilization process well in advance; often at the same time they begin the resource mobilization process. Early planning for demobilization facilitates accountability and makes transportation of resources as efficient as possible--both in terms of costs and time of delivery.

TRACKING AND REPORTING RESOURCES

Resource tracking is a standardized, integrated process conducted throughout the life-cycle of an incident by all agencies at all levels. This process provides incident managers with a clear picture of where resources are located, helps staff prepare to receive resources, protects the safety of personnel and security of supplies and equipment, and enables the coordination of movement of personnel, equipment, and supplies.

Resource managers use established procedures to track resources continuously from mobilization through demobilization. Ideally, these managers would display this real-time information in a centralized database accessible to all NIMS partners, allowing total visibility of assets. Managers follow all required procedures for acquiring and managing resources, including reconciliation, accounting, auditing, and inventorying.

RECOVERING RESOURCES

Recovery involves the final disposition of all resources. During this process, resources are rehabilitated, replenished, disposed of, and retrograded.

NON-EXPENDABLE RESOURCES

These resources are fully accounted for at the incident site and again when they are returned to the unit that issued them. The issuing unit then restores the resources to fully functional capability and readies them for the next mobilization. Broken and/or lost items should be replaced through the Supply Unit, by the entity with invoicing responsibility for the incident, or as defined in pre-incident agreements. In the case of human resources, such as Incident Management Teams (IMTs), adequate rest and recuperation time and facilities are provided. Mobilization guides developed at each jurisdictional level and within functional agencies provide appropriate rest and recuperation time guidelines. Important occupational health and mental health issues must also be addressed, including monitoring how such incidents affect emergency responders over time.

EXPENDABLE RESOURCES

These resources are also fully accounted for. Restocking occurs at the point from which a resource was issued. The incident management organization bears the costs of expendable resources, as authorized in preplanned financial agreements concluded by preparedness organizations. Returned resources that are not in restorable condition—whether expendable or non-expendable—must be declared as excess according to established regulations and policies of the controlling entity. Waste management is of special note in the process of recovering resources. Resources that require special handling and disposition (e.g., biological waste and contaminated supplies, debris, and equipment) are dealt with according to established regulations and policies.

REIMBURSEMENT

Reimbursement provides a mechanism to recoup funds expended for incident-specific activities. Reimbursement processes also play an important role in establishing and maintaining the readiness of resources. Processes and procedures must be in place to ensure that resource providers are reimbursed in a timely manner. These must include mechanisms for collecting bills, validating costs against the scope of the work, ensuring that proper authorities are involved, and accessing reimbursement programs, such as the Public Assistance Program and the Emergency Relief Program.

COMPONENT IV

COMMAND AND MANAGEMENT

The previous components of the NIMS—Preparedness, Communications and Information Management, and Resource Management—provide a framework to facilitate clear response authority, resource acquisition, and effective management during incident response. The Incident Command System (ICS), multi-agency coordination systems (MACS), and Public Information Systems (PIS) are the fundamental elements of the NIMS that direct incident operations; acquire, coordinate, and deliver resources to incident sites; and share information about the incident with the public, respectively. Taken together, these elements of Command and Management are the most visible aspects of incident management, typically executed with a sense of urgency.

This component describes the systems used to facilitate incident command and management operations, including the Incident Command System, Multi-Agency Coordination System, and Public Information Systems.

INCIDENT COMMAND SYSTEM

The ICS is a widely applicable management system designed to enable effective and efficient incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. ICS is a fundamental form of management established in a standard format with the purpose of enabling incident managers to identify the key concerns associated with the incident (often times under urgent conditions) without sacrificing attention to any component.

The ICS can be viewed as a "tool box" from which incident managers may choose all or some applicable "tools" necessary to fulfill their functional roles in a full range of incidents and events. The NIMS also provides standardization through established organization structures (ICS, Multi-agency Coordination System, and Public Information System) and consistent terminology. These choices allow for similar incidents to be managed using different tools.

ICS is used to organize both near-term and long-term field-level operations for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade. As a system, the ICS is extremely useful: not only does it provide an organizational structure for incident management; it also

guides the process for planning, building, and adapting that structure. Utilizing ICS on every incident or planned event helps hone and maintain skills needed for the large-scale incidents.

The ICS is used by all levels of government—Federal, State, local, and Tribal—as well as by many private sector and nongovernmental organizations. The ICS is also applicable across disciplines. It is normally structured to facilitate activities in five major functional areas: (1) Command, (2) Operations, (3) Planning, (4) Logistics, and (5) Finance and Administration.

Acts of biological, chemical, radiological, and nuclear terrorism represent particular challenges for the traditional ICS structure. Incidents that are not site specific, are geographically dispersed, or evolve over longer periods of time will require extraordinary coordination among all participants including Federal, State, Tribal, local, private sector, and NGOs. An area command may be established to oversee the management of such incidents.

CONCEPTS AND PRINCIPLES

NON-DISRUPTIVE IMPLEMENTATION

Effective implementation of ICS will have minimal disruption on existing systems and processes. This will facilitate its acceptance across a nationwide user community and to insure continuity in the transition process from normal operations.

USER-FRIENDLY AND APPLICABLE SYSTEM

ICS should be user friendly and applicable across a wide spectrum of emergency response and incident management disciplines. This will enable the communication, coordination, and integration critical to create an effective and efficient system.

LOCAL INCIDENT MANAGEMENT

Most incidents are managed locally. The initial response to most incidents is typically handled by local "911" dispatch centers, emergency responders within a single jurisdiction, and direct supporters of emergency responders. Most responses need go no further. In other instances, incidents that begin with a single response discipline within a single jurisdiction may rapidly expand to multi-discipline, multi-jurisdictional incidents requiring significant additional resources and operational support. Whether for incidents which additional resources are required or are provided from different organizations within a single jurisdiction or outside the jurisdiction, or for complex incidents with national implications (such as an emerging infectious disease or a bioterror attack), the ICS provides a flexible core mechanism for coordinated and collaborative incident management. When a single incident covers a large geographical

area, multiple local ICS organizations may be required. Effective cross-jurisdictional coordination using processes and systems is absolutely critical in this instance.

STANDARD ORGANIZATION, DOCTRINE, AND PROCEDURES

The NIMS requires that field command and management functions be performed in accordance with a standard set of ICS organizations, doctrine, and procedures; furthermore, the ICS allows for the flexibility to modify procedures or organizational structure to align as necessary with the operating characteristics of their specific jurisdictions or to accomplish the mission in the context of a particular hazard scenario.

MODULAR AND SCALABLE

ICS is designed to be modular and scalable with the following operating characteristics:

- suitable for operations within a single jurisdiction or single agency, a single jurisdiction with multi-agency involvement, or multiple jurisdictions with multi-agency involvement;
- applicable and acceptable to users throughout the country;
- readily adaptable to new technology;
- adaptable to any emergency or incident to which incident management agencies would be expected to respond; and
- flexible within a scalable organizational structure, based on the size and complexity of the incident.

INTERACTIVE MANAGEMENT COMPONENTS

ICS has interactive management components that set the stage for effective and efficient incident management and emergency response.

COMMON TERMINOLOGY, STANDARDS, AND PROCEDURES

ICS establishes common terminology, standards, and procedures that enable diverse organizations to work together effectively. These include a standard set of pre-designated organizational elements and functions, common names for resources used to support incident operations, common "typing" for resources to reflect specific capabilities, and common identifiers for facilities and operational locations used to support incident operations.

MEASURABLE OBJECTIVES

ICS incorporates measurable objectives that ensure fulfillment of incident management goals. Establishing objectives begins at the top and is communicated throughout the entire organization.

MANAGEMENT CHARACTERISTICS

ICS is based on 14 proven management characteristics, each of which contributes to the strength and efficiency of the overall system. These characteristics are: (1) Common Terminology, (2) Modular Organization, (3) Managements by Objectives, (4) Reliance on Incident Action Plan, (5) Manageable Span of Control, (6) Pre-designated Incident Facilities and Locations, (7) Comprehensive Resource Management, (8) Integrated Communications, (9) Establishment and Transfer of Command, (10) Chain of Command and Unity of Command, (11) Unified Command, (12) Accountability, (13) Deployment, and (14) Information & Intelligence Management.

COMMON TERMINOLOGY

ICS establishes common terminology that allows diverse incident management and support entities to work together across a wide variety of incident management functions and hazard scenarios. This common terminology covers the following:

ORGANIZATIONAL FUNCTIONS

Major functions and functional units with incident management responsibilities are named and defined. Terminology for the organizational elements involved is standard and consistent.

RESOURCE DESCRIPTIONS

Major resources—including personnel, facilities, and major equipment and supply items—used to support incident management activities are given common names and are "typed" with respect to their capabilities, to help avoid confusion and to enhance interoperability.[32]

INCIDENT FACILITIES

Common terminology is used to designate the facilities in the vicinity of the incident area that will be used during the course of incident management.

[32] See page 81. Ongoing Management and Maintenance, NIMS Integration Center for more on resource typing.

MODULAR ORGANIZATION

The incident command organizational structure develops in a top-down, modular fashion that is based on the size and complexity of the incident, as well as the specifics of the hazard environment created by the incident. When needed, separate functional elements can be established, each of which may be further subdivided to enhance internal organizational management and external coordination. Responsibility for the establishment and expansion of the ICS modular organization ultimately rests with Incident Command, who base the ICS organization on the requirements of the situation. As incident complexity increases, the organization expands from the top down as functional responsibilities are delegated. Concurrently with structural expansion, the number of management and supervisory positions expands to adequately address the requirements of the incident.

THE INCIDENT ACTION PLAN (IAP) IS BUILT ON P-O-S-T:

P – Priorities. Regardless of the size or complexity of an event or incident the priorities remain constant

O – Objectives. Broad descriptions or statements of the desired outcomes or actions to achieve consistent with the priorities

S – Strategies. Action processes by which the objectives are met

T – Tactics (or Tasks). Specific activities that are implemented to achieve the identified strategies

MANAGEMENT BY OBJECTIVES

Management by objectives represents an approach that is communicated throughout the entire ICS organization. This approach includes the following:

- establishing overarching incidents objectives;
- developing strategies based on overarching incident objectives;
- developing and issuing assignments, plans, procedures, and protocols;
- establishing specific, measurable tactical objectives for various incident management functional activities, and directing efforts to attain them, in support of defined strategies; and
- documenting results to measure performance and facilitate corrective action.

RELIANCE ON AN INCIDENT ACTION PLAN

Incident action plans (IAPs) provide a concise and coherent means of capturing and communicating the overall incident priorities, objectives and strategies in the contexts of both operational and support activities.

A typical, incident or event may not require the preparation of a written IAP. Most initial response operations are not captured with a formal IAP. However if an incident is likely to extend beyond one operational period, become more complex or involve multiple entities, preparation of a written IAP will become increasingly important to maintain effective, efficient and safe operations.

MANAGEABLE SPAN OF CONTROL

Span of control is key to effective and efficient incident management. Within ICS, the span of control of any individual with incident management supervisory responsibility should range from three to seven subordinates, with the optimum being five. The type of incident, nature of the task, hazards and safety factors, and distances between personnel and resources all influence span-of-control considerations.

PRE-DESIGNATED INCIDENT FACILITIES AND LOCATIONS

Various types of operational support facilities are established in the vicinity of an incident dependent on the size and complexity to accomplish a variety of purposes, such as staging, decontamination, donated goods processing, and mass care. The Incident Commander (IC) will direct the identification and location of facilities based on the requirements of the situation at hand. Typical pre-designated facilities include incident command posts, bases, camps, staging areas, mass casualty triage areas, recovery supply Points-of-Distribution (POD) sites, and others, as required.

COMPREHENSIVE RESOURCE MANAGEMENT

Maintaining an accurate and up-to-date picture of resource utilization is a critical component of incident management. Resource management includes processes for identifying, listing, categorizing, typing, ordering, dispatching, tracking, and recovering resources. It also includes processes to facilitate reimbursement for resources, as appropriate. Resources are defined as personnel, teams, equipment, supplies, and facilities available or potentially available for assignment or allocation in support of incident management and emergency response activities.

INTEGRATED COMMUNICATIONS

Incident communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures. This integrated approach links the operational and support units of the various agencies involved and are necessary to maintain communications connectivity and discipline and enable common situational awareness and interaction. Preparedness planning must address the equipment, systems, and protocols necessary to achieve integrated voice and data incident management communications.

ESTABLISHMENT AND TRANSFER OF COMMAND

The command function must be clearly established from the beginning of incident operations. The agency with primary jurisdictional authority over the incident designates the individual at the scene

responsible for establishing command. When command is transferred, the process must include a briefing that captures all essential information for continuing safe and effective operations.

Chain of Command and Unity of Command

Chain of command refers to the orderly line of authority within the ranks of the incident management organization. Unity of command means that every individual has a designated supervisor to whom they report at the scene of the incident. These principles clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers at all levels must be able to control the actions of all personnel under their supervision.

Unified Command

In incidents involving multiple jurisdictions, a single jurisdiction with multi-agency involvement, or multiple jurisdictions with multi-agency involvement, unified command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.

Accountability

Effective accountability at all jurisdictional levels and within individual functional areas during incident operations is essential. To that end, the following principles must be adhered to:

CHECK-IN

All responders, regardless of agency affiliation, must report in to receive an assignment in accordance with the procedures established by the IC.

INCIDENT ACTION PLAN

Response operations must be directed and coordinated as outlined in the IAP.

UNITY OF COMMAND

Each individual involved in incident operations will be assigned to only one supervisor.

PERSONAL RESPONSIBILITY

All responders are expected to be personally responsible for their actions.

SPAN OF CONTROL

Supervisors must be able to adequately supervise and control their subordinates, as well as communicate with and manage all resources under their supervision.

RESOURCE TRACKING

Supervisors must record and report resource status changes as they occur.

DISPATCH/DEPLOYMENT

Resources should respond only when requested or when dispatched by an appropriate authority through established resource management systems. Available but not requested resources must refrain from spontaneous deployment in order to prevent the overburdening of the recipient and compounding accountability challenges. Resources, including supplies, should only be dispatched upon appropriate authority and through established resource management systems.

INFORMATION AND INTELLIGENCE MANAGEMENT

The incident management organization must establish a process for gathering, analyzing, sharing, and managing incident-related information and intelligence.

ICS ORGANIZATION AND OPERATIONS

COMMAND AND GENERAL STAFF OVERVIEW

The ICS organization has five major functions.[33] These are: command, operations, planning, logistics, and finance and administration (with a potential sixth functional area to cover the information and intelligence management function, as described in paragraph above).

COMMAND

Command encompasses Incident Commander (IC) and their Command Staff. This may be exercised as a single Incident Commander or under Unified Command (UC). In cases where multiple site-specific IC or UC systems are established an Area Command may also be established to support and integrate the management efforts of the multiple IC and/or UC systems. Command Staff positions may be established to assign/delegate responsibility for command activities that the IC or UC members cannot perform due to the complexity of the incident or other situational demands. These positions may include the Public Information Officer (PIO), Safety Officer (SO), and Liaison Officer (LNO), in addition to various others, as required and assigned by the IC.

[33] Summary table of major ICS positions is contained in Appendix C.

GENERAL STAFF

General Staff encompasses incident management personnel who represent the major functional elements of the ICS including the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief. Command Staff and General Staff must continually interact and share vital information and estimates of the current and future situation and develop recommended courses of action for consideration by the IC.

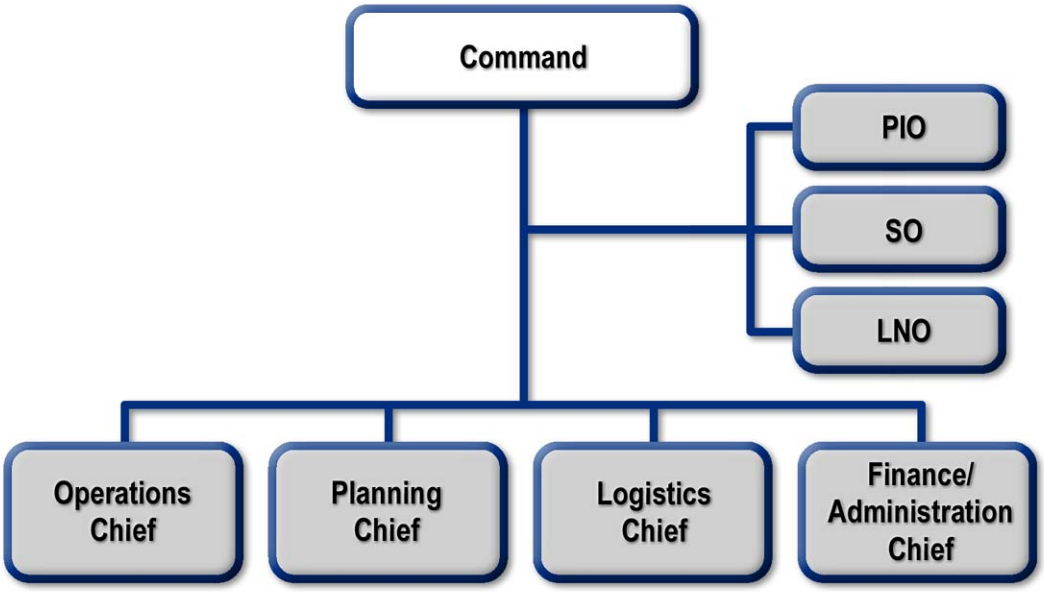


Figure 4—Incident Command System: Command Staff and General Staff

INCIDENT MANAGEMENT TEAMS

An Incident Management Team (IMT) is an incident command organization made up of the command and general staff members, and appropriate functional units, in an ICS organization. National, State, and some local IMTs have formal certification and qualification, notification, deployment, and operational procedures in place. In other cases, ad hoc IMTs are formed at incident or for specific events. The level of training and experience of the IMT members, coupled with the identified formal response requirements and responsibilities of the IMT, are factors in determining the "Type", or level, of IMT.

INCIDENT COMMAND AND COMMAND STAFF

Incident Command is responsible for overall management of the incident. This includes Command Staff assignments required to support the command function. The Command and General Staffs are typically located at the Incident Command Post (ICP).

INCIDENT COMMAND

The command function may be conducted in two general ways:

SINGLE INCIDENT COMMANDER

When an incident occurs within a single jurisdiction and there is no jurisdictional or functional agency overlap, a single IC should be designated with overall incident management responsibility by the appropriate jurisdictional authority. (In some cases in which incident management crosses jurisdictional and/or functional agency boundaries, a single IC may be designated if all parties agree to such an option.) Jurisdictions should consider pre-designating ICs in their preparedness plans.

The designated IC will develop the incident objectives on which subsequent incident action planning will be based. The IC will approve the Incident Action Plan (IAP) and all requests pertaining to the ordering and releasing of incident resources.

UNIFIED COMMAND

Unified Command (UC) is an important element in multi-jurisdictional or multi-agency incident management. It provides guidelines to enable agencies with different legal, geographic, and functional responsibilities to coordinate, plan, and interact effectively. As a team effort, UC allows all agencies with jurisdictional authority or functional responsibility for the incident, to jointly provide management direction to an incident through a common set of incident objectives and strategies established at the command level. Each participating agency maintains its authority, responsibility, or accountability.

ADVANTAGES OF USING UNIFIED COMMAND

- A single set of objectives is developed for the entire incident
- A collective approach is used to develop strategies to achieve incident objectives
- Information flow and coordination is improved between all jurisdictions and agencies involved in the incident
- All agencies with responsibility for the incident have an understanding of joint priorities and restrictions
- No agency's legal authorities will be compromised or neglected
- The combined efforts of all agencies are optimized as they perform their respective assignments under a single Incident Action Plan

Unified Command functions as a single integrated management organization. This means:

- co-located command at ICP;
- one Operations Section Chief to direct tactical efforts;
- a coordinated process for resource ordering; and
- shared planning, logistical, and finance/administration operations, wherever possible.

All agencies in the UC structure contribute to the process of:

- determining overall incident strategies;

- selecting objectives;
- ensuring that joint planning for tactical activities is accomplished in accordance with approved incident objectives;
- ensuring the integration of tactical operations; and
- approving, committing, and making optimum use of all assigned resources.

The exact composition of the UC structure will depend on the location(s) of the incident (i.e., which geographical administrative jurisdictions are involved) and the type of incident (i.e., which functional agencies of the involved jurisdiction(s) are required). In the case of some multi-jurisdictional incidents, the designation of a single IC may be considered to promote greater unity of effort and efficiency.

The designated agency officials participating in the UC represent different legal authorities and functional areas of responsibility and use a collaborative process to establish, identify, and rank incident priorities and determine appropriate objectives consistent with the priorities. Agencies heavily involved in the incident that lack jurisdictional responsibility are defined as supporting and/or assisting agencies. They are represented to the command structure and effect coordination on behalf of their parent agency through the Liaison Officer. Jurisdictional responsibilities of multiple incident management officials are consolidated into a single planning process, including:

- responsibilities for incident management;
- incident objectives;
- resource availability and capabilities;
- limitations; and
- areas of agreement and disagreement between agency officials.

Incidents are managed under a single, collaborative approach, including the following:

- common organizational structure;
- single incident command post;
- unified planning process; and
- unified resource management.

Under UC, the IAP is developed by the Planning Section and is approved by the UC. A single individual, the Operations Section Chief, directs the tactical implementation of the IAP. The Operations Section Chief will normally come from the agency with the greatest jurisdictional involvement. UC participants will agree on the designation of the Operations Section Chief.

Unified Command works best when the participating members of the UC co-locate at the Incident Command Post and observe the following practices:

- select an Operations Section Chief for each operational period;
- keep each other informed of specific requirements;

- establish consolidated incident objectives, priorities, and strategies;
- coordinate to establish a single system for ordering resources;
- develop a consolidated IAP, written or oral, evaluated and updated at regular intervals; and
- establish procedures for joint decision-making and documentation.

Table 3—Difference between Single IC and UC

PRIMARY DIFFERENCES BETWEEN A SINGLE INCIDENT COMMANDER AND UNIFIED COMMAND	
Single Incident Commander	Unified Command
The IC is solely responsible (within the confines of his or her authority) for establishing incident objectives and strategies. The IC is directly responsible for ensuring that all functional area activities are directed toward accomplishment of the strategy.	The individuals designated by their jurisdictional authorities (or by departments within a single jurisdiction) must jointly determine objectives, strategies, plans, resource allocations, and priorities and work together to execute integrated incident operations and maximize the use of assigned resources.

COMMAND STAFF

In an incident command organization, the Command Staff consists of Incident Command and various special staff positions. The special staff positions are specifically designated, report directly to Incident Command, and are assigned responsibility for key activities that are not a part of the ICS General Staff functional elements. Three special staff positions are typically identified in ICS: Public Information Officer, Safety Officer, and Liaison Officer. Additional positions may be required, depending on the nature, scope, complexity, and location(s) of the incident(s), or according to specific requirements established by the IC.

PUBLIC INFORMATION OFFICER (PIO)

The PIO is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements. The PIO develops accurate and complete information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external consumption. The PIO may also perform a key public information-monitoring role. Whether the command structure is single or unified, only one incident PIO should be designated. Assistants may be assigned from other agencies or departments involved. The IC must approve the release of all incident-related information.

SAFETY OFFICER (SO)

The SO monitors incident operations and advises Incident Command on all matters relating to operational safety, including the health and safety of emergency responder personnel. The ultimate responsibility for the safe conduct of incident management operations rests with the IC or UC and supervisors at all levels of incident management. The SO is, in turn, responsible to Incident Command for the set of systems and procedures necessary to ensure ongoing assessment of hazardous environments, coordination of multi-agency safety efforts, and implementation of measures to promote emergency responder safety, as well as the general safety of incident operations. The SO has emergency authority to stop and/or prevent unsafe acts during incident operations. In a UC structure, a single SO should be designated, in spite of the fact that multiple jurisdictions and/or functional agencies may be involved. Assistants may be required and may be assigned from other agencies or departments constituting the UC. The SO, Operations Section Chief, and Planning Section Chief must coordinate closely regarding operational safety and emergency responder health and safety issues. The SO must also ensure the coordination of safety management functions and issues across jurisdictions, across functional agencies, and with the private sector and NGOs. It is important to note that the agencies, organizations, or jurisdictions that contribute to joint safety management efforts do not lose their individual identities or responsibility for their own programs, policies, and personnel. Rather, each entity contributes to the overall effort to protect all responder personnel involved in incident operations.

LIAISON OFFICER (LNO)

The LNO is Incident Command's point of contact for representatives of other governmental agencies, NGOs, and/or private entities (with no jurisdiction or legal authority), to provide input on their agency's policies, resource availability, and other incident related matters. In either a single IC or UC structure, representatives from assisting or cooperating agencies and organizations coordinate through the LNO. Agency and/or organizational representatives assigned to an incident must have the authority to speak for their parent agencies and/or organizations on all matters, following appropriate consultations with their agency leadership. Assistants and personnel from other agencies or organizations (public or private) involved in incident management activities may be assigned to the LNO to facilitate coordination.

ADDITIONAL COMMAND STAFF

Additional Command Staff positions may also be necessary depending on the nature and location(s) of the incident, and/or specific requirements established by Incident Command. For example, a Legal Counsel may be assigned directly to the Command Staff to advise Incident Command on legal matters, such as emergency proclamations, legality of evacuation orders, and legal rights and restrictions pertaining to media access. Similarly, a Medical Advisor—an agency operational medical dispatcher or assigned physician, may be designated and assigned directly to the Command Staff to provide advice and recommendations to Incident Command in the context of incidents involving medical and mental health services, mass casualty, acute care, vector control, epidemiology, and/or mass prophylaxis considerations, particularly in the response to a bioterrorism incident.

LOCATION OF INCIDENT COMMAND AND COMMAND STAFF

The tactical-level, on-scene incident command and management organization is located at the Incident Command Post (ICP). Incident Command directs operations from the ICP, which is generally located at or in the immediate vicinity of the incident site. Typically, there is one ICP established for each incident. Depending on the number and location of incidents, there may be multiple IMTs managed by an Area Command. As Federal, State, Tribal, and local responders deploy, they must, regardless of agency affiliation, report in to the designated, assembly, marshalling or staging area and notify the IC or UC to receive an assignment in accordance with the procedures established by the IC or the UC.

GENERAL STAFF

The General Staff represents and is responsible for the functional aspects of the incident command structure. The General Staff typically consists of the chiefs of the Operations, Planning, Logistics, and Finance/Administration Sections, which are discussed more fully below.

OPERATIONS SECTION

This section is responsible for all activities focused on reduction of the immediate hazard, saving lives and property, establishing situational control, and restoration of normal operations. Lifesaving and responder safety will always be the highest priorities and the first objectives in the incident action plan (IAP).

Figure 5 depicts the organizational template for an Operations Section. Expansions of this basic structure will vary according to numerous considerations and operational factors. In some cases, the organizational structure will be determined by jurisdictional boundaries. In other cases, a strictly functional approach will be used. In still others, a mix of functional and geographical considerations may be appropriate. The ICS offers flexibility in determining the right structural approach for the specific circumstances of the incident at hand.

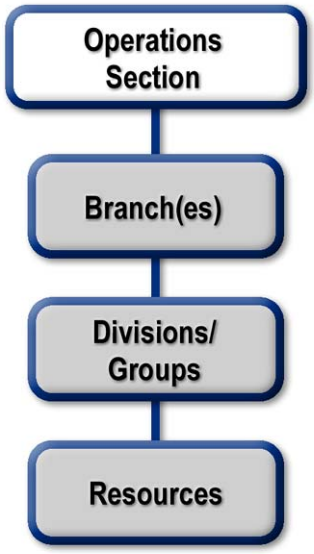


Figure 5—Major Organizational Elements of Operations Section

OPERATIONS SECTION CHIEF

The Operations Section Chief is responsible to Incident Command or UC for the direct management of all incident-related operational activities. The Operations Section Chief will establish tactical objectives for the assigned operational period, with other section chiefs and unit leaders establishing their own supporting objectives. The Operations Section Chief may have one or more deputies assigned, with the assignment of deputies from other agencies encouraged in the case of multi-jurisdictional incidents. An Operations Section Chief should be designated for each operational period and should have direct involvement in the preparation of the IAP.

BRANCHES

Branches may be used to serve several purposes, and may be functional, geographic or both depending on the circumstances of the incident. In general, Branches are established when the number of divisions or entities s exceeds the recommended span of control.

DIVISIONS AND GROUPS

Divisions and Groups are established when the number of resources exceeds the manageable span of control of Incident Command and the Operations Section Chief. Divisions are established to divide an incident into physical and/or geographical areas of operation. Groups are established to divide the incident into functional areas of operation. For certain types of incidents, for example, Incident Command may assign evacuation or mass care responsibilities to a functional group in the Operations Section. There also may be additional levels of supervision below the Division or Group level.

RESOURCES

Resources refer to personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or an EOC. Resources may be organized and managed in three different ways, depending on the requirements of the incident:

- *Single Resources.* These are individual personnel, supplies and equipment items, and the operators associated with them.
- *Task Forces.* A Task Force is any combination of resources assembled in support of a specific mission or operational need. All resource elements within a Task Force must have common communications and a designated leader.
- *Strike Teams.* Strike Teams are a set number of resources of the same kind and type that have an established minimum number of personnel. All resource elements within a Strike Team must have common communications and a designated leader. The use of Strike Teams and Task Forces is encouraged, wherever possible, to optimize the use of resources, reduce the span of control over a large number of single resources, and reduce the complexity of incident management coordination and communications.

PLANNING SECTION

The Planning Section collects, evaluates, and disseminates incident situation information and intelligence to Incident Command and incident management personnel, prepares status reports, displays situation information, maintains status of resources assigned to the incident, and develops and documents the IAP, based on guidance from Incident Command.

As shown in Figure 6, the Planning Section comprises four primary units, as well as a number of technical specialists to assist in evaluating the situation, developing planning options, and forecasting requirements for additional resources.

The Planning Section is normally responsible for gathering and disseminating information and intelligence critical to the incident, unless Incident Command places this function elsewhere.

The Planning Section is also responsible for developing and documenting the IAP. The IAP includes the overall incident objectives and strategies established by Incident Command. In the case of UC, the IAP

must adequately address the mission and policy needs of each jurisdictional agency, as well as interaction between jurisdictions, functional agencies, and private organizations. The IAP also addresses tactical objectives and support activities required for one operational period, generally 12 to 24 hours.

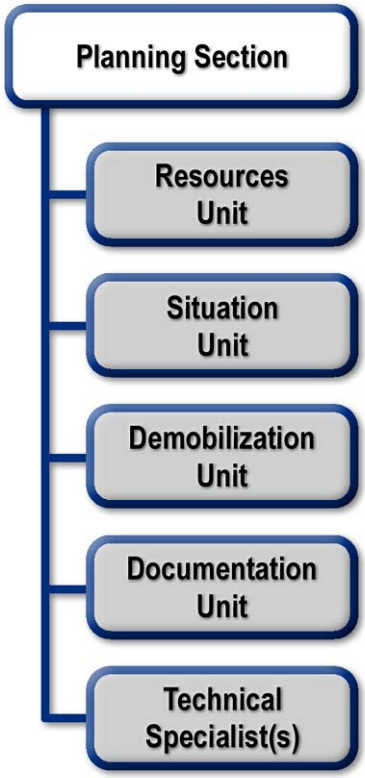


Figure 6—Planning Section Organization

The IAP should incorporate changes in strategies and tactics based on lessons learned during earlier operational periods. A written IAP is especially important when:

- resources from multiple agencies and/or jurisdictions are involved;
- multiple jurisdictions are involved;
- the incident will effectively span several operational periods;
- changes in shifts of personnel and/or equipment are required; or
- there is a need to document actions and/or decisions.

The IAP will typically contain a number of components, as shown in Table 4.

Table 4—Sample IAP Outline

COMPONENTS	NORMALLY PREPARED BY
Incident Objectives (Form: ICS 202)	Incident Commander
Organization List or Chart (Form: ICS 203)	Resources Unit
Assignment List (Form: ICS 204)	Resources Unit
Communications Plan (Form: ICS 205)	Communications Unit
Responder Medical Plan (Form: ICS 206)	Medical Unit
Incident Map	Situation Unit
General Safety Message	Safety Officer
OTHER POTENTIAL COMPONENTS (INCIDENT DEPENDENT)	
Air Operations Summary	Air Operations
Traffic Plan	Ground Support Unit
Decontamination Plan	Technical Specialist
Waste Management or Disposal Plan	Technical Specialist
Demobilization Plan	Demobilization Unit
Evacuation Plan	Technical Specialist
Site Security Plan	Law Enforcement Technical Specialist or Security Manager
Investigative Plan	Law Enforcement Technical Specialist
Evidence Recovery Plan	Law Enforcement Technical Specialist
Evacuation/Sheltering Plan	As Required
Other	

LOGISTICS SECTION

The Logistics Section (see Figure 7) is responsible for all support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. It also provides facilities, security, transportation, supplies, equipment maintenance and fuel, food services, communications and information technology support, and emergency responder medical services, including inoculations, as required.

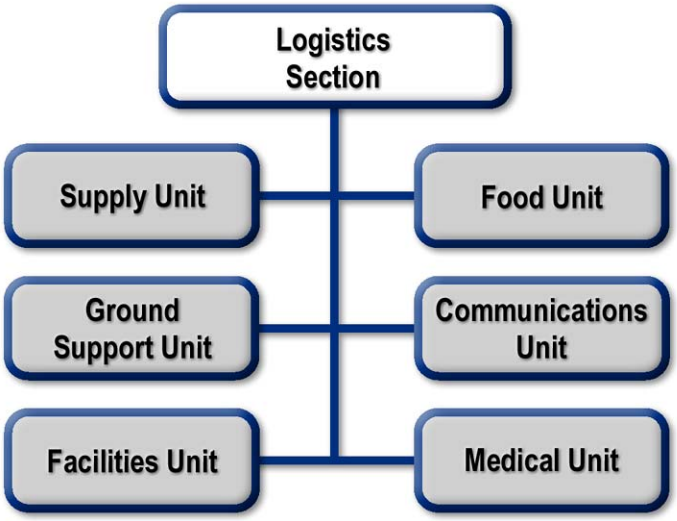


Figure 7—Logistics Section Organization

FINANCE/ADMINISTRATION SECTION

A Finance/Administration Section is established when the agency(s) involved in incident management activities require(s) finance and other administrative support services. Not all incidents will require a separate Finance/Administration Section in the ICP. In the majority of incidents, the components of Finance/Administration may be better managed or performed in a location separate from the ICP. In cases that require only one specific function (e.g., cost analysis); this service may be provided by a technical specialist in the Planning Section. The basic organizational structure for a Finance/Administration Section is shown in Figure 8. When such a section is established, the depicted units may be created, as required.

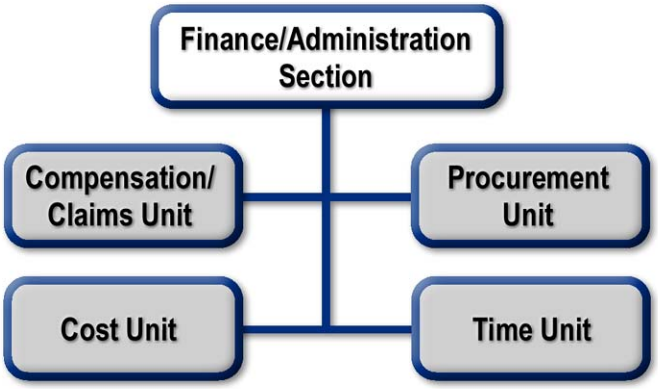


Figure 8—Finance and Administration Section Organization

INFORMATION AND INTELLIGENCE FUNCTION

The analysis and sharing of information and intelligence are important elements of ICS. The incident management organization must establish a process for collecting, analyzing, and using incident-related information and intelligence for decision support. In this context, intelligence includes not only national security or other types of classified information but also other operational information, such as risk assessments, medical intelligence (e.g., surveillance), weather information, geospatial data, structural designs, toxic contaminant levels, and utilities and public works data that may come from a variety of different sources. Traditionally, information and intelligence functions are located in the Planning Section. However, in exceptional situations, Incident Command may need to assign the information and intelligence functions to other parts of the ICS organization. In any case, information and intelligence must be appropriately analyzed and shared with personnel, designated by Incident Command, who have proper clearance and a "need-to-know" to ensure that they support decision-making.

The intelligence and information function may be organized in one of the following ways:

- Within the Command Staff

  This option may be most appropriate in incidents with little need for tactical or classified intelligence and in which incident-related intelligence is provided by supporting Agency Representatives, through real-time reach-back capabilities.

- As a Unit within the Planning Section

  This option may be most appropriate in an incident with some need for tactical intelligence and when no law enforcement entity is a member of the UC.

- As a Branch within the Operations Section

This option may be most appropriate in incidents with a high need for tactical intelligence (particularly classified intelligence) and when law enforcement is a member of the UC.

- As a Separate General Staff Section

  This option may be most appropriate when an incident is heavily influenced by intelligence factors or when there is a need to manage and/or analyze a large volume of classified or highly sensitive intelligence or information. This option is particularly relevant to a terrorism incident, for which intelligence plays a crucial role throughout the incident life-cycle.

Regardless of how it is organized, the information and intelligence function is also responsible for developing, conducting, and managing information-related security plans and operations as directed by Incident Command. These can include information security and operational security activities, as well as the complex task of ensuring that sensitive information of all types (e.g., classified information, sensitive law enforcement information, proprietary and personal information, or export-controlled information) is handled in a way that not only safeguards the information but also ensures that it gets to those who need access to it so that they can effectively and safely conduct their missions. The information and intelligence function also has the responsibility for coordinating information-and-operational-security matters with public awareness activities that fall under the responsibility of the PIO, particularly where such public awareness activities may affect information or operations security.

INCIDENT COMPLEX - MULTIPLE INCIDENT MANAGEMENT WITH A SINGLE ICS ORGANIZATION

DESCRIPTION

An Incident Complex is two or more individual incidents located in the same general proximity, which are assigned to a single IMT or UC. When an Incident Complex is established over several individual incidents, the general guideline is that the previously identified incidents would become Branches within the Operations Section of the IMT. This provides more potential for future expansion if required. The reason for this is that more flexibility is then available within each branch to later establish divisions or groups if required. Also, because divisions and groups may already have been established at each of the incidents, the same basic structure can be carried on. If any of the incidents within a complex has potential to become a large-scale incident, it is best to establish it as a separate incident with its own ICS organization. If the number of incidents exceeds the span of control for the agency(ies), Area Command can be utilized.

Examples where a complex model may be used:

- An earthquake, tornado, flood, etc., where there are many separate incidents occurring in close proximity.
- Several separate fires are burning in close proximity to one another.

- One incident is underway with an IMT assigned and other smaller incidents occur in the same proximity.

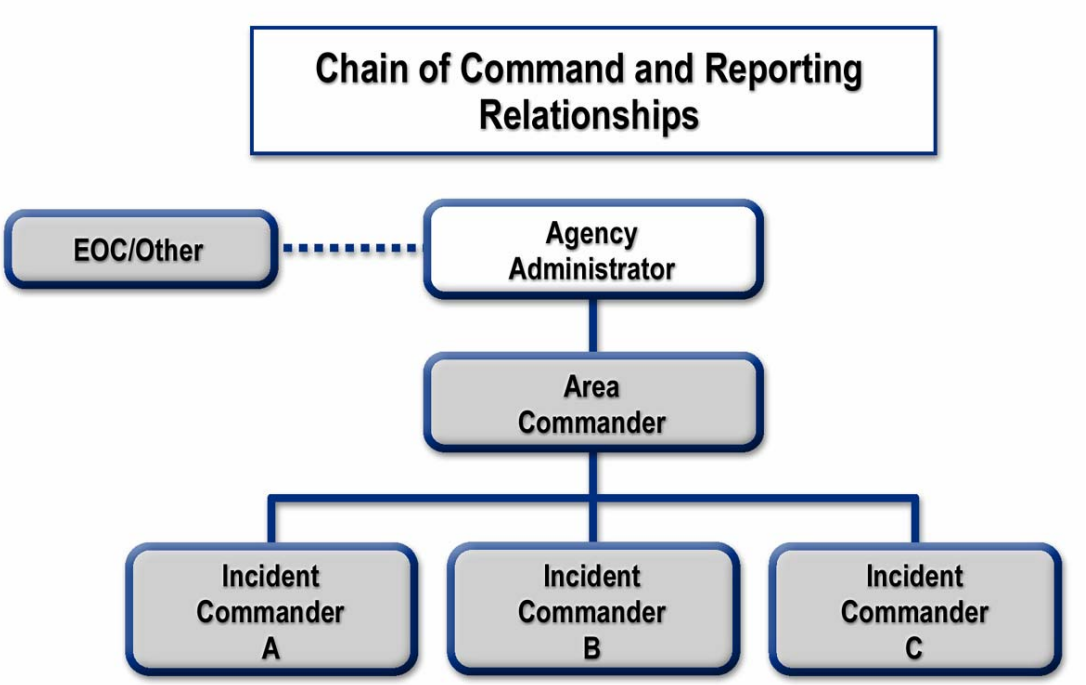
Considerations for the use of a complex:

- A complex may be managed under a single command or a UC.
- The incidents are close enough to be managed by the same IMT.
- Some staff and/or logistical support economies could be achieved through a combined management approach.
- The number of overall incidents within the jurisdiction requires consolidations wherever possible to conserve staff and reduce costs.
- Planning, Logistical, and Finance/Administration activities can be adequately provided to the complex from a single management team.

AREA COMMAND

DESCRIPTION

An Area Command is activated only if necessary, depending on the complexity of the incident and incident management span-of-control considerations. An agency administrator or other public official with jurisdictional responsibility for the incident usually makes the decision to establish an Area Command. An Area Command is established either to oversee the coordination of multiple incidents that are each being handled by a separate ICS organization or to oversee the management of a very large incident that involves multiple ICS organizations (see Figure 9), such as would likely be the case for incidents that are not site specific, geographically dispersed, or evolve over longer periods of time, (e.g., a bioterrorism incident). In this sense, acts of biological, chemical, radiological, and/or nuclear terrorism represent particular challenges for the traditional ICS structure and will require extraordinary coordination between Federal, State, local, Tribal, private sector, and nongovernmental organizations. Area Command is also used when there are a number of incidents in the same area and of the same type, such as two or more hazardous material (HAZMAT) or oil spills, and fires. These represent incidents that may compete for the same resources. When incidents do not have similar resource demands, they are usually handled separately and are coordinated through an EOC. If the incidents under the authority of the Area Command are multi-jurisdictional, then a Unified Area Command should be established. This allows each jurisdiction to have representation in the command structure. Area Command should not be confused with the functions performed by an EOC. An Area Command oversees and coordinates the incident(s), while an EOC coordinates support functions and provides resources support.



*The dotted line connecting EOC/Other with the Agency Administrator represents the link between an EOC and an Agency Administrator. This connection is meant to show coordination between the two, not a direct link within the chain of command.

Figure 9—Chain of Command and Reporting Relationships in an Area Command

RESPONSIBILITIES

For incidents under its authority, an Area Command has the responsibility to

- set overall incident-related priorities;
- allocate critical resources according to priorities;
- ensure that incidents are properly managed;
- ensure that incident management objectives are met and do not conflict with each other or with agency policy;
- identify critical resource needs and report them to EOCs and/or multi-agency coordination entity; and
- ensure that short-term emergency recovery is coordinated to assist in the transition to full recovery operations.

ROLE OF ELECTED AND APPOINTED OFFICIALS DURING AN INCIDENT

Generally, elected and appointed officials are not at the scene of the incident, but must have the ability to communicate and meet with Incident Command as necessary. Depending on the nature of the incident or level of the overall emergency, elected and appointed officials could function from the following locations:

- the agency or jurisdiction offices;
- an EOC; or
- a Multi-agency Coordination Entity (either as a functional agency representative, or representing a political subdivision).

MAJOR RESPONSIBILITIES OF THE ELECTED AND APPOINTED OFFICIALS:

- clearly state the agency/jurisdiction's policy;
- evaluate effectiveness and correct deficiencies; and
- support a multi-agency approach.

Elected and appointed officials provide policy, mission, direction and authority to Incident Command. Proper coordination between elected and appointed officials and Incident Command can be crucial to successful management of an incident and will best serve the public.[34]

Elected and appointed officials must clearly communicate views to Incident Command. As time and agency policy dictate, the following considerations should be documented and provided to Incident Command, preferably through a formal delegation of authority:

- cost considerations;
- environmental issues;
- legal and policy restraints and/or freedoms;
- limitations on authority;
- issues relating to critical infrastructure services or restoration;
- economic, political, and social concerns; and
- safety considerations.

[34] ICS courses are available for Elected and Appointed Officials (e.g. G402, Incident Command System (ICS) *Overview for Executives/Senior Officials*).

MULTI-AGENCY COORDINATION SYSTEMS

Multi-agency coordination is a process that allows all levels of government and all disciplines to work together more efficiently and effectively. Multi-agency coordination occurs across the different disciplines involved in incident management, across jurisdictional lines or across levels of government. Examples of where multi-agency coordination can occur include but are not limited to an incident scene, within the Area command structure, at an EOC, etc.

**MACS IS A SYSTEM…
NOT SIMPLY A FACILITY**

One of the key elements within the process is the multi-agency coordination system (MACS). It is a system that agencies adopt in order to efficiently work together, planning and coordinating resources and other support for preplanned, notice or no-notice events. MACS define business practices, standard operating procedures, processes, and protocols by which participating agencies will coordinate their interactions. An integral element of a jurisdiction's MACS are their dispatch procedures and protocols, incident command structure and the coordination and support activities taking place within an activated EOC.

Written agreements allow agencies within a MACS to conduct activities using established rules and are oftentimes self-defined by the participating organizations. MACS are adaptive to the coordination of multi-agency resources at a small incident, within and between EOCs, Incident Management Teams (IMT) and Area Commands, and other Multi-agency Coordination Entities (MACE).[35] A fully implemented MACS is critical for seamless multi-agency coordination activities and is essential to the success and safety of the response, whenever more than one jurisdictional agency responds. Moreover, the use of MACS is one of the fundamental components of Command and Management within the NIMS, as it promotes scalability and flexibility necessary for a coordinated response.

DEFINITION

A multi-agency coordination system is an activity or formal system consisting of any combination of facilities, equipment, personnel, procedures, practices and communications integrated into a common system with the purpose of coordinating resources and support between diverse agencies and jurisdictions. A MACS operates as a support function and generally does not communicate on a direct

[35] For the purpose of this document multi-agency coordination entity and multi-agency coordination group are interchangeable terms.

basis with Incident Command. Direct tactical and operational responsibility for conducting incident management activities rests with Incident Command. During some incidents, the IC may communicate directly with the MACS for the purpose of requesting resources, providing situational information, clarifying policy, or other assistance such as legal counsel. In turn MACS may communicate directly with the IC to provide feedback and essential guidance for situations not specifically addressed in pre-incident planning.

The primary functions of a MACS are to:

- support incident management policies and priorities;
- facilitate logistics support and resource tracking;
- establish and communicate resource allocation priority decisions;
- coordinate incident related information; and
- coordinate inter-agency and inter-governmental activities regarding incident management policies, priorities, and strategies.

SYSTEM ELEMENTS

Emergency responders and public safety personnel respond to a variety of incidents on a daily basis all of which require multi-agency coordination. While ad-hoc arrangements among agencies may ultimately be effective, multi-agency coordination is most successful when it takes place within a pre-planned and established multi-agency coordination system.

EXAMPLES OF MULTI-AGENCY COORDINATION

Multi-agency coordination during emergency response and recovery efforts may take place at several levels and within various forms of command and coordination systems. For example:

At Incident Scene: Agencies routinely work together and coordinate within an ICS structure at an incident. The intent, design, and structure of ICS incorporate and promote the concept of multi-agency coordination.

MACS can be set up:
- at a jurisdictional EOC
- at a regional facility
- at a State or Federal facility
- wherever it is needed

Multi-agency coordination entities consist of:
- people who make the MACS function
- representatives authorized to commit agency resources and funds

At Area Command: An Area Command, once established with command authority for several incidents in the same proximity, is responsible for coordinating inter-agency matters related to those incidents.

At Dispatch Center: Agencies and the ICS structure at an incident routinely work together with an coordinate with the Dispatch Center. The Dispatch Center can serve as a primary coordination and support element of the MACS for an incident until other element of MACS are formally established.

At Departmental Operations Center (DOC): Agencies within a political jurisdiction may establish coordination, communications, control, logistics, etc at the departmental levels for conducting overall emergency management of their assigned resources for local incidents. DOCs normally focus on internal agency incident management and response and are linked to and, in most cases, are physically represented in a combined agency EOC by authorized agent(s) for the department or entity.

At Emergency Operations Center (EOC): Jurisdictional Emergency Operations Centers with assigned representatives from appropriate departments and liaison agencies often support multi-agency coordination. Jurisdictional EOCs may even serve the role of multi-agency coordination entity.

At Regional Level: Multi-agency Coordination may take place by bringing together representatives from various jurisdictions and functional agencies to coordinate in an inter-jurisdictional regional setting. The requirement for this level of coordination increases in proportion to the complexity and number of incidents. Many states have regions or other subdivisions which bring State and local agencies together when incidents cross jurisdictional boundaries.

At State and Federal Levels - Federal and State emergency management organizations routinely work together to assist the emergency response and disaster recovery efforts of local, State and Federal agencies. This type of coordination takes place at the state's EOC, a Regional Response Coordination Center (RRCC), and/or a Joint Field Offices (JFO).

At National EOCs: At the Federal level the FEMA National Response Coordination Center (NRCC) and the National Operations Center (NOC) are examples of what could be considered a national level EOC. Other departments and agencies may also have EOCs at this level. Another group such as the Domestic Readiness Group (DRG) can be activated as needed to address issues that cannot be resolved at lower levels, provide strategic policy direction, and set priorities and allocate scarce resources at a national level and better fits the definition of a national MAC Entity than a national EOC.

MULTI-AGENCY COORDINATION: SIMPLE TO COMPLEX

The complexity of the MAC System is dependent on the type, size, complexity, and probable duration of incident operations.

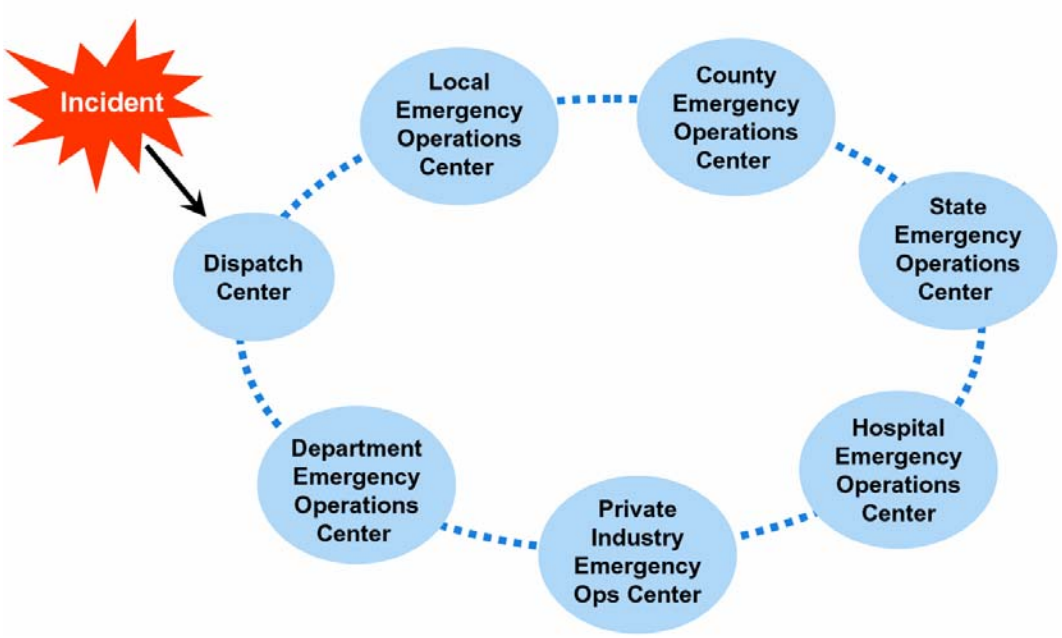


Figure 10—Multi-agency Coordination: Simple to Complex

EMERGENCY OPERATIONS CENTER

The most common and familiar form of a MACS is an EOC. EOCs may be permanent organizations and facilities that are staffed 24 hours a day seven days a week or may be established to meet temporary, short-term needs. The Incident Command Post (ICP) is located at or in the immediate vicinity of an incident site and is primarily focused on the tactical on-scene response. In smaller-scale incidents or during the initial phase of the response to larger incidents, the ICP may perform in an EOC-like capacity. Standing EOCs, or those activated to support larger, more complex incidents, are typically established in a more central or permanently established facility, at a higher level of organization within a jurisdiction.

EOCs may be organized by major discipline (fire, law enforcement, medical services, etc); by jurisdiction (city, county, region, etc); by emergency support function (communications, public works and engineering, transportation, resource support, etc); or, more likely, by some combination thereof. ICPs should also be linked to EOCs to ensure effective and efficient incident management.

EOCs may be permanent organizations and facilities or may be established to meet temporary, short-term needs.

For complex incidents, EOCs may be staffed by personnel representing multiple jurisdictions and functional disciplines and a wide variety of resources. For example, a local EOC established in response to a bioterrorism incident would likely include a mix of law enforcement, emergency management, public health, and medical personnel (representatives of health care facilities, pre-hospital emergency medical services, patient transportation systems, pharmaceutical repositories, laboratories, etc.).

The physical size, staffing, and equipping of an EOC will depend on the size of the jurisdiction, resources available and anticipated incident management workload. EOCs may be organized and staffed in a variety of ways. Regardless of the specific organizational structure used, EOCs should include the following core functions: coordination; communications; resource dispatch and tracking; and information collection, analysis, and dissemination.

On activation of a local EOC, communications and coordination must be established between Incident Command and the EOC, when they are not co-located. ICS field organizations must also establish communications with the activated local EOC, either directly or through their parent organizations. Additionally, EOCs at all levels of government and across functional agencies must be capable of communicating appropriately with other EOCs during incidents, including those maintained by private organizations. Communications between EOCs must be reliable and contain built-in redundancies. The efficient functioning of EOCs most frequently depends on the existence of mutual-aid agreements and joint communications protocols among participating agencies.[36]

EOC IS ACTIVATED:
- To support the on site response during an escalating incident by relieving the burden of external coordination and securing additional resources

EOC IS:
- A physical location
- Staffed with personnel trained for and authorized to represent their agency/discipline
- Equipped with mechanisms for 2-way communications with the incident site and to alert and obtain resources and potential resources
- Managed through protocols
- Applicable at different levels of government

EOC CONSISTS OF:
- Personnel and equipment appropriate for the level of incident

EOC IS USED:
- In varying ways within all levels of government and the private-sector
- To provide coordination, direction, and support during emergencies

EOC MAY:
- Facilitate MACS functions and may be needed to support Area Command, IC or UC when resource needs exceed local capabilities

EOC DOES NOT:
- Command at the field level of the incident

[36] Such agreements are also discussed in Component I: Preparedness, *Mutual-Aid Agreements*. Page 21.

MULTI-AGENCY COORDINATION ENTITIES

When incidents cross disciplinary or jurisdictional boundaries or involve complex incident management scenarios, a multi-agency coordination entity (MAC entity and MAC group are used interchangeably), such as an emergency management agency, may be used to facilitate incident management and policy coordination. The situation at hand and the needs of the jurisdictions involved will dictate how these MAC entities conduct their business, as well as how they are structured. MAC entities typically consist of principals (or their designees) from organizations and agencies with direct incident management responsibility or with significant incident management support or resource responsibilities. These entities are sometimes referred to as a MAC-entity action teams, policy committees, incident management groups, executive teams, or other similar terms. In some instances, EOCs may serve a dual function as a multi-agency coordination entity; in others, the preparedness organizations discussed in Component I may fulfill this role. Regardless of the term or organizational structure used, these entities typically provide strategic coordination during domestic incidents. If constituted separately, multi-agency coordination entities, preparedness organizations, and EOCs must coordinate and communicate with one another to provide uniform and consistent guidance to incident management personnel.

Regardless of form or structure, the principal functions and responsibilities of multi-agency coordination entities typically include the following:

- ensuring that each agency involved in incident management activities is providing appropriate situational awareness and resource status information;
- establishing priorities between incidents and/or Area Commands in concert with Incident Command involved;
- acquiring and allocating resources required by incident management personnel in concert with the priorities established by Incident Command;
- anticipating and identifying future resource requirements;
- coordinating and resolving policy issues arising from the incident(s); and
- providing strategic coordination as required.

Following incidents, multi-agency coordination entities are also typically responsible for ensuring that improvements in plans, procedures, communications, staffing, and other capabilities necessary for improved incident management are acted on. These improvements should also be coordinated with appropriate preparedness organizations, if these organizations are constituted separately.[37]

[37] These organizations are discussed in Component I: Preparedness, *Preparedness Organizations.* Page 11.

PRIMARY FUNCTIONS OF MULTI-AGENCY COORDINATION SYSTEMS

Multi-agency coordination systems should be both flexible and scalable, to best contribute to efficient and effective incident management. There are common functions that MACS will generally perform during an incident response. Consistent with the concepts of flexibility and scalability, though, not all MACS functions will be performed during every incident and may not occur in any particular order.

SITUATION ASSESSMENT

Situation assessment is the collection, processing, and display of all information needed by the multi-agency coordination entity. This may take the form of consolidating agency/jurisdiction situation reports, obtaining supplemental information, and preparing maps and status boards.

CRITICAL RESOURCE ACQUISITION AND ALLOCATION

Designated critical resources will be acquired if possible from the involved agencies or jurisdictions. Agencies or jurisdictions may shift resources internally to match priority needs as a result of multi-agency coordination entity decisions. Resources available from incidents in the process of demobilization may be shifted to higher priority incidents, etc.

Resources may also be acquired from outside the affected area. Procedures for acquiring outside resources will vary depending upon the agencies involved, pre-existing mutual-aid agreements, the involvement of State and Federal resources, etc.

COORDINATION WITH ELECTED AND APPOINTED OFFICIALS

A primary function of the multi-agency coordination entity will be to assist coordination among elected and appointed officials at all levels of government. This is an extremely important part of the multi-agency coordination entity responsibilities, as the allocation of scarce resources away from one agency's or jurisdiction's incident(s) to another of higher priority will obviously require immediate and close coordination with the officials of the affected jurisdiction(s).

COORDINATION OF SUMMARY INFORMATION

By virtue of its situation assessment function, the MACS may provide summary information on incidents within its area of responsibility, and provide agency/jurisdictional contacts for media and other interested agencies. The systems to accomplish the communication to the media and others are covered in the Public Information section.

INCIDENT PRIORITY DETERMINATION

Establishing the priorities among ongoing incidents within the defined area of responsibility is another primary function of the multi-agency coordination entity. Typically, a multi-agency coordination entity will coordinate with Area and/or Incident Command to prioritize the incident demands specified by Command. Additional considerations determining priorities include:

- Life threatening situations
- Real property threatened

- High damage potential
- Incident complexity
- Environmental impact
- Economic impact
- Other criteria established by the multi-agency coordination entity/group[38]

Table 5—Differences between a Multi-Agency Coordination Entity and Area Command

MULTI-AGENCY COORDINATION ENTITY	AREA COMMAND
Off-site coordination and support system	On-site command function of the Incident Command System. Area command may be established as Unified Area Command
Members are agency administrators or designees from the agencies involved or heavily committed to the incident	Members are the most highly skilled incident management personnel
Organization generally consists of the Multi-agency coordination entity (agency administrators), Multi-agency coordination entity Coordinator, and an intelligence and information support staff	Organization generally consists of an Area Commander, Assistant Area Commander—Planning, and Assistant Area Commander—Logistics
Is the agency administrator or designee	Is delegated authority for specific incident(s) from the agency administrator
Allocate and reallocate critical resources through the dispatch system by setting incident priorities	Assign and reassign critical resources allocated to them by MAC or the normal dispatch system organization
Make coordinated agency administrator level decisions on issues that affect multiple agencies	Ensure that incident objectives and strategies are complimentary between Incident Management Teams

[38] M-480, Multi-agency Coordinating Group Training Course. National Wildfire Coordination Group. 2007, http://www.na.fs.fed.us/firetraining/trngsched.htm.

LEVELS OF MULTI-AGENCY COORDINATION

The following depicts examples of multi-agency coordination occurring at several levels of operation.

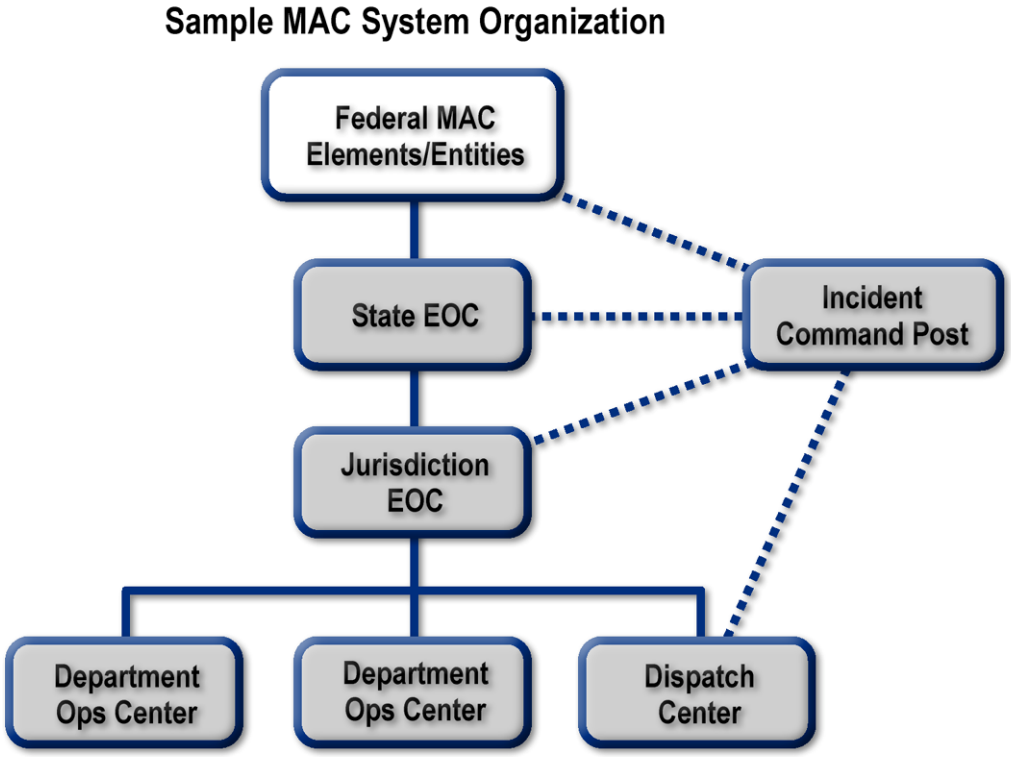


Figure 11—Sample MAC System Organization

PUBLIC INFORMATION SYSTEMS

INTRODUCTION

Public Information Systems are used to communicate timely and accurate information to the public and responders before, during, and after incidents. Well developed public information strategies and communications plans ensure life saving measures, evacuation routes, threat and alert systems and other public safety information is coordinated and communicated to numerous audiences. Public Information

Systems provide processes, procedures and organizational structure to implement information strategies and plans, at all levels of government during an incident.

SYSTEM DESCRIPTION AND COMPONENTS

PUBLIC INFORMATION OFFICER AND INCIDENT COMMAND

Under the ICS, the PIO is a key staff member supporting the incident command structure. The PIO represents and advises Incident Command on all public information matters relating to the management of the incident. The PIO handles media and public inquiries, emergency public information and warnings, rumor monitoring and response, media monitoring, and other functions required to coordinate, clear with appropriate authorities, and disseminate accurate and timely information related to the incident, particularly regarding information on public health and safety and protection. The PIO is also responsible for coordinating public information at or near the incident site and serving as the on-scene link to the Joint Information System (JIS). In a large-scale operation, the on-scene PIO serves as a field PIO with links to the Joint Information Center (JIC), which is typically co-located with the Federal, regional, State, local, or Tribal EOC tasked with primary incident coordination responsibilities. The JIS provides the mechanism for ensuring consistent messaging and integrating public information activities among JIC's, across jurisdictions, and with the private sector and NGOs.

ROLES OF PUBLIC INFORMATION OFFICERS

The PIO develops accurate and complete information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external use.

JOINT INFORMATION SYSTEM

The JIS provides an organized, integrated, and coordinated mechanism to ensure the delivery of understandable, timely, accurate, and consistent information to the public in a crisis. It includes the plans, protocols, and structures used to provide information to the public during incident operations, and encompasses all public information operations related to an incident, including all Federal, State, local, Tribal and private entity PIOs, staff, and JICs established to support an incident. Key elements include the following:

- inter-agency coordination and integration;
- developing and delivering coordinated messages;
- support for decision-makers; and
- flexibility, modularity, and adaptability.

JOINT INFORMATION CENTER

A JIC is a physical location where personnel with public information responsibilities from organizations involved in incident management activities can co-locate to perform critical emergency-information, crisis-communications, and public-affairs functions. Typically an incident-specific JIC is established at a single, on-scene location, in coordination with State and local agencies depending on the requirements of the incident or at the national level if the situation warrants. An incident-specific JIC develops, coordinates, and disseminates unified news releases. News releases are cleared through Incident Command, the Emergency Operations Center, and/or Federal officials in the case of national incidents, to ensure consistent messages, avoid release of conflicting information, and prevent negative impact on operations. This formal approval process for news releases ensures protection of law enforcement-sensitive information or other sensitive but unclassified information. Agencies may issue their own news releases related to their policies, procedures, programs, and capabilities; however, these should be coordinated with an incident-specific JIC. In most incidents where a JIC is established, the government lead will be appointed by the IC or UC with concurrence from agency administrators.

POSSIBILITY OF A VIRTUAL JIC

A Joint Information Center may involve real-time, constant links to other sites, thus creating a virtual JIC. Advantages of a virtual JIC are more rapid establishment of all appropriate participation in the JIC and expanded resources of a "home office" site being part of the JIC. Any virtual links should be fully integrated into the JIC so that it functions as a single-site operation.

A National JIC may be used when an incident requiring Federal coordination is expected to be of a long duration (i.e., weeks or months) and when the incident affects a large area of the country.

- The JIC must include representatives of each jurisdiction, agency, private sector, and nongovernmental organization involved in incident management activities.
- A single JIC location is preferable, but the system should be flexible and adaptable enough to accommodate virtual or multiple JIC locations when the circumstances of an incident require. Multiple JICs may be needed for a complex incident spanning a wide geographic area or multiple jurisdictions.
- Each JIC must have procedures and protocols to communicate and coordinate effectively with other JICs, as well as with other appropriate components of the ICS organization.
- Liaisons may establish and maintain mutual understanding and cooperation among participating entities

An example of typical JIC organization is shown in Figure 12.

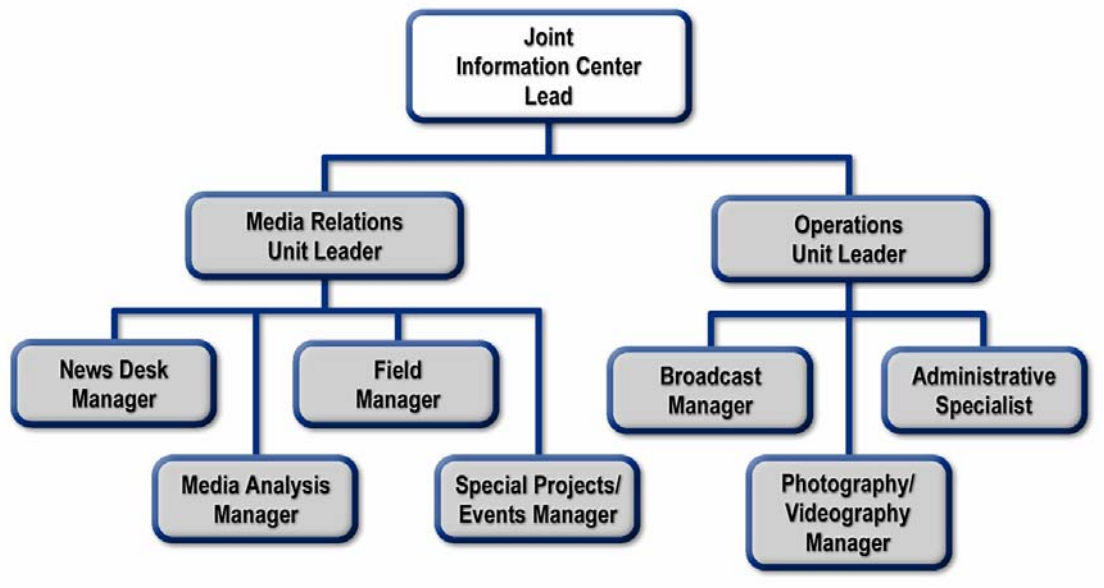


Figure 12—Joint Information Center Organization

In light of the need for real-time communications, JICs can be organized in many ways, depending on the nature of the incident. Table 6 identifies several types of JICs.

Table 6—Types of Joint Information Centers

INCIDENT	• Optimal physical location for local and incident assigned PIOs to co-locate • Easy media access is paramount to success
VIRTUAL	• Used when physical co-location is not feasible • Uses technology and communication protocols
SATELLITE	• Smaller in scale than other JICs • Established primarily to support the Incident JIC
AREA	• Supports wide-area multiple incident ICS structures • Media access is paramount • Could be established on a State-wide basis
NATIONAL	• Established for long duration incidents • Established to support a Federal response activities • Staffed by numerous Federal departments and/or agencies

ORGANIZATIONAL INDEPENDENCE

Organizations participating in incident management retain their independence. Incident Command and multi-agency coordination systems are responsible for establishing and overseeing JICs including processes for coordinating and clearing public communications. In the case of UC, the departments, agencies, organizations, or jurisdictions that contribute to joint public information management do not lose their individual identities or responsibility for their own programs or policies. Rather, each entity contributes to the overall unified message.

COORDINATION OF PUBLIC INFORMATION

Public Information functions must be coordinated and integrated across jurisdictions and across functional agencies; among Federal, State, local, and Tribal partners; and with the private sector and NGOs. During emergencies, the public may receive information from a variety of sources. The JIC provides a location for organizations participating in the management of an incident to work together to ensure that timely, accurate, easy-to-understand, and consistent information is disseminated to the public. The JIC comprises representatives from each entity involved in the management of an incident. In large or complex incidents, particularly those involving complex medical and public health information requirements, JICs may be established at various levels of government. All JICs must communicate and coordinate with each other on an ongoing basis. Public awareness functions must also be coordinated with the information- and operational-security matters that are the responsibility of the information and intelligence function of the ICS, particularly when public awareness activities may affect information or operations security.

COMMUNICATION PLANNING

Communication planning is essential to ensure rapid response. Maintaining draft news releases, media lists, contact information of political officials and leads of public service organizations will facilitate the dissemination of emergency public information to numerous audiences. Training and exercising must incorporate communications as an operational component.

Integrated at the local, Tribal, State, and Federal levels management of communications with the public is the approach used to manage communications with the public during incidents requiring a coordinated response. Management of communications with the public incorporates the following processes:

- CONTROL: Identification of key roles and release authority of the primary and supporting departments and agencies responding to the incident.
- COORDINATION: Specification of interagency coordination and plans, notification, activation, and supporting protocols. A decision regarding the location and structure of the JIC requires coordination and is an important factor in operational planning.

- COMMUNICATIONS: Development of message content such as incident facts, health risk concerns, pre-incident and post-incident preparedness recommendations, warnings issues, incident information, messages, audiences, and strategies for when, where, how, and by whom the messages will be delivered.

FEDERAL COMMUNICATION PROTOCOLS

In accordance with the National Response Plan, pre-identified incident communications protocols are established and ready for use during any incident requiring a coordinated Federal response. Dedicated incident communications lines have been identified to aid communications between different levels of government.[39] These lines are explained in Table 7 below.

Table 7—Communication Lines and Protocols

National Incident Communications Conference Line (NICCL)	• Transmits and exchanges critical and timely [e.g., "breaking"] incident information among Federal and affected State, local, and Tribal public affairs and public information personnel. • During sustained incident management activity, the NICCL will be used for daily or other incident communications coordination calls.
State Incident Communications Coordination Line (SICCL)	• Similar dedicated Federal-State incident communications conference line • Facilitates and assures the inclusion, transmission, and exchange of incident management information, evacuee coordination, and messaging relating to all States and territories. • Examples: Unclassified public affairs guidance supporting threat information or status changes, pending national decisions, and major incidents where updates are beneficial in support of State-Federal external affairs situational awareness.
Private Sector Incident Communications Coordination Line (PICCL)	• Standing line for use by Critical Infrastructure/Key Resources (CI/KR) incident communications coordinators. • Access information will be coordinated and disseminated by DHS Infrastructure Protection and DHS Public Affairs. • During an incident requiring a coordinated Federal response, the Office of Public Affairs works with DHS/OIP and the Assistant Secretary for the Private Sector to provide timely public information to the CI/KR sectors and their members, for dissemination as necessary to their members.

[39] For further information see ESF 15 – External Affairs Annex to the NRP.

RELATIONSHIPS AMONG COMMAND AND MANAGEMENT ELEMENTS

The ICS, MACS, and Public Information Systems have been described here as separate elements of command and management within the NIMS. However, the NIMS relies on the relationships among these elements along with the elements themselves.

Some relationships are specifically defined. For example, an Area Command or Incident Command coordinates with the PIS on incident-specific public information by placing an incident PIO within the JIS, typically located at a JIC. The relationship between Area Command or Incident Command and MACS is primarily defined by a communications link between Command and/or incident-site resource managers and a particular staff position within a multi-agency coordination entity.

These relationships—along with other relationships among command and management elements that are not as clearly defined in advance—must be clearly defined and documented as each system evolves during an incident.

ONGOING MANAGEMENT AND MAINTENANCE

NIMS INTEGRATION CENTER

HSPD-5 required the Secretary of Homeland Security to establish a mechanism for ensuring the ongoing management and maintenance of the NIMS.[40] To this end, the Secretary established a multi-jurisdictional, multi-disciplinary NIMS Integration Center (NIC), designated to serve as an asset for government agencies at all levels, the private sector and NGOs who are implementing the NIMS. The NIC provides strategic direction for and oversight of the NIMS, supporting both routine maintenance and continuous refinement of the system and its components over the long term. The NIC will include mechanisms for direct participation from and/or regular consultation with other Federal departments and agencies; State, local, and Tribal incident management entities; emergency responder and incident management professional organizations; and private sector and nongovernmental organizations.

The NIC is also responsible for the continued development of a process for ongoing revisions and updates to the NIMS. Revisions to the NIMS and other corrective actions can be proposed by:

- local entities (including their preparedness organizations);
- State entities (including their preparedness organizations);
- regional entities (including their preparedness organizations);
- Tribal entities (including their preparedness organizations);
- Federal departments and agencies;

[40] FY2007 DHS Appropriations Bill, PL 109-295, Section 509. "SEC. 509. NATIONAL INTEGRATION CENTER. (a) In General.—There is established in the Agency a National International Center. (b) Responsibilities.— (1) In General.—The Administrator, through the National Integration Center, and in consultation with other Federal departments and agencies and the National Advisory Council, shall ensure ongoing management and maintenance of the National Incident Management System, the National Response Plan and any successor to such system or plan."

- private entities (including businesses, volunteer organizations, academia, and other nonprofit and NGOs); and
- NIMS-related professional associations.

CONCEPTS AND PRINCIPLES

The process for managing and maintaining the NIMS ensures that all users and stakeholders—including various levels of government, functional disciplines, and private entities—are given the opportunity to participate in NIC activities. To accomplish this goal, the NIC is multi-jurisdictional and multi-disciplinary and maintains appropriate liaison with private organizations.

The NIMS management and maintenance process relies heavily on lessons learned from actual incidents and incident management training and exercises, as well as recognized best practices across jurisdictions and functional disciplines.

NIMS REVISION PROCESS

Proposed changes to the NIMS will be submitted to the NIC for consideration, approval, and publication. The Secretary has ultimate authority and responsibility for publishing revisions and modifications to NIMS-related documents, including supplementary standards, procedures, and other materials, in coordination with other Federal, State, local, Tribal, and private entities with incident management and emergency responder responsibilities, expertise, and experience. The NIC will periodically release upgraded versions of the NIMS document, typically following coordination with stakeholders from all levels of government, private sector and NGOs.

NIC RESPONSIBILITIES

ADMINISTRATION AND COMPLIANCE

To manage ongoing administration and implementation of NIMS, including specification of compliance measures, the NIC is responsible for working toward:

- developing a national program for NIMS education and awareness, including specific instruction on the purpose and content of this document and the NIMS in general;
- promoting compatibility between national-level standards for the NIMS and those developed by other public, private, and/or professional groups; and
- facilitating the establishment and maintenance of a documentation and database system related to qualification, certification, and credentialing of incident management personnel and organizations, including reviewing and approving (in coordination with national professional organizations and with input from the Federal, State, Tribal, local, private sector and nongovernmental entities), as appropriate, of the discipline-specific requirements submitted by functionally oriented incident management organizations and associations;
- developing assessment criteria for the various components of the NIMS, as well as compliance requirements and compliance timelines for Federal, State, local, and Tribal entities regarding NIMS standards and guidelines; and
- integrating into the national R&D agenda, in coordination with the Under Secretary for Science and Technology of the Department of Homeland Security, the incident management science and technology needs of departments, agencies, disciplines, the private sector, and NGOs operating within the NIMS.

STANDARDS AND CREDENTIALING

The NIC will work with appropriate standards development organizations (SDOs) to ensure the adoption of common national standards and credentialing systems that are compatible and aligned with the implementation of the NIMS. Identification, adoption, and development of common standards and credentialing system include:

- facilitating the development and publication of national standards, guidelines, and protocols for the qualification and certification of emergency responder and incident management personnel, as appropriate;
- reviewing and approving (with the assistance of national professional organizations and with input from Federal, State, local, Tribal, private sector, and non-governmental entities), as appropriate, the

discipline-specific qualification and certification requirements submitted by emergency responder and incident management organizations and associations;

- establishing a data maintenance system to provide incident managers with the detailed qualification, experience, and training information needed to credential personnel for prescribed "national" incident management positions;
- coordinating minimum professional certification standards and facilitation of the design and implementation of a credentialing system that can be used nationwide;
- facilitating the establishment of standards for the performance, compatibility, and interoperability of incident management equipment and communications systems, including the following:
  - facilitating, in coordination with appropriate Federal agencies, standards-making, certifying, and accrediting organizations, and appropriate State, local, Tribal, private sector, and nongovernmental organizations, the development and/or publication of national standards, guidelines, and protocols for equipment certification (including the incorporation of standards and certification programs already in existence and used by incident management and emergency response organizations nationwide)
  - reviewing and approving (in coordination with national professional organizations and with input from Federal, State, local, Tribal, private sector, and nongovernmental entities) lists of equipment that meet these established equipment certification requirements
  - collaborating with organizations responsible for emergency responder equipment evaluation and testing
- facilitating the development and issuance of national standards for the typing of resources;
- facilitating the definition and maintenance of the information framework required to guide the development of NIMS information systems, including the development of data standards for the following: incident notification and situation reports, status reporting, analytical data, geospatial information, wireless communications, identification and authentication, and incident reports, including lessons learned reports; and
- coordinating the establishment of technical and technology standards for NIMS users in concert with the Under Secretary for Science and Technology of the Department of Homeland Security and recognized SDOs.

The NIC recommends that State and local governments ***voluntarily adopt*** the following National Fire Protection Association (NFPA) standards: NFPA 1600 and NFPA 1561.[41] The following table illustrates the links between these two recommended standards and their appropriate NIMS components:

[41] The National Fire Protection Association, "NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs," 2004 Edition; and "NFPA 1561: Standard on Emergency Services Incident Management System," 2005 Edition. Standards such as these are regularly reviewed and updated to maintain currency.

1 Table 8—NFPA Standards and NIMS

PROPOSED STANDARD	NIMS COMPONENTS	TOPICS COVERED
NFPA 1600	Component I – Preparedness	Section 5: • Preparedness hazard and risk assessment. • Hazard mitigation strategy. • Resource management planning and objectives. • Mutual aid planning. • Emergency operations and control planning. • Public awareness and communications planning. • Financial planning.
NFPA 1561	Component II – Communications and Information Management	Section 6: • Communications systems. Section 7: • Management and control of communications systems.
NFPA 1600	Component II – Communications and Information Management	Section 5: • General communications systems and procedures. • Public awareness and communications.
NFPA 1600	Component III – Resource Management	Section 5: • Resource management and mutual aid planning. Annex C: • Listing of additional mutual aid resources to consider.
NFPA 1600	Component IV – Command and Management	Section 4: • Program management. • Advisory committee for interagency

		coordination. • Program evaluation. Section 5: • Essential program elements to command and management. • Business continuity issues.
NFPA 1561	Component IV – Command and Management	Section 4: • Risk assessment and management in incident command functions. Section 7: • Incident action plans. • Accountability. • Emergency management and control. • Span of control. • Command and general staffing. • Incident command functions. • Multi-agency coordination. Section 8: • Multi-agency involvement and coordination.

TRAINING AND EXERCISE SUPPORT

To lead development of training and exercises that further appropriate agencies and organizations knowledge, adoption, and implementation of the NIMS, the NIC will coordinate with them to:

- facilitate the definition of general training requirements and the development of national-level training standards and course curricula associated with the NIMS, including the following:
  - the use of modeling and simulation capabilities for training and exercise programs
  - field-based training, specification of mission-essential tasks, requirements for specialized instruction and instructor training, and course completion documentation for all NIMS users
  - the review and recommendation (in coordination with national professional organizations and Federal, State, local, Tribal, private sector, and nongovernmental entities) of discipline-specific NIMS training courses;

- facilitate the development of national standards, guidelines, and protocols for incident management training and exercises, including consideration of existing exercise and training programs at all jurisdictional levels; and
- establish and maintain a repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, as well as for best practices, model structures, and model processes for NIMS-related functions.

PUBLICATION MANAGEMENT

Publication management for the NIMS includes development of naming and numbering conventions; review and certification of publications; methods for publications control; identification of sources and suppliers for publications and related services; and management of publication distribution.

NIMS publication management includes the following types of products:

- qualifications information;
- training course and exercise information;
- task books;
- ICS training and forms;
- other necessary forms;
- job aids;
- guides;
- computer programs;
- audio and video resources;
- templates; and
- "best practices."

To manage publications related to the NIMS, the NIC will coordinate with appropriate agencies and organizations and take the lead on:

- facilitating the establishment and maintenance of a publication management system for documents supporting the NIMS and other NIMS-related publications and materials, including the development or coordination of general publications for all NIMS users, as well as their issuance via a NIMS publication management system;
- facilitating the development and publication of materials (such as supplementary documentation and desk guides) and standardized templates to support implementation and continuous refinement of the NIMS; and

- reviewing (in coordination with appropriate national professional standards-making, certifying, and accrediting organizations and with input from Federal, State, local, Tribal, private sector and nongovernmental entities) of the discipline-specific publication management requirements submitted by professional organizations and associations.

SUPPORTING TECHNOLOGIES

As the NIMS and its supporting systems evolve to be more flexible, scalable, and reliable, incident managers and coordinating units will increasingly rely upon new technology and technological systems to implement and continuously refine NIMS. Technologies include voice and data communications systems, information systems (e.g., record keeping and resource tracking), and display systems. These also include specialized technologies that facilitate incident operations and incident management activities in situations that call for unique technology-based capabilities.

Ongoing development of science and technology is integral to continual improvement and refinement of the NIMS. Strategic research and development (R&D) ensures that this development takes place. The NIMS also relies on scientifically based technical standards that support the nation's ability to prepare for, prevent, respond to, and recover from incidents. Maintaining an appropriate focus on science and technology solutions as they relate to incident management will necessarily involve a long-term collaborative effort among NIMS partners.

CONCEPTS AND PRINCIPLES

The NIMS leverages science and technology to improve capabilities and lower costs. It observes five key principles:

INTEROPERABILITY AND COMPATIBILITY

Systems must be able to work together and should not interfere with one another if the multiple jurisdictions, organizations, and functions that come together under the NIMS are to be effective in incident management. Interoperability and compatibility are achieved through the use of such tools as common communications and data standards, digital data formats, equipment standards, and design standards.

TECHNOLOGY SUPPORT

Technology support permits organizations using the NIMS to enhance all aspects of incident management and emergency response. Technology support facilitates incident operations and sustains

the research and development (R&D) programs that underpin the long-term investment in the nation's future incident management capabilities.

TECHNOLOGY STANDARDS

Supporting systems and technologies are based on requirements developed through preparedness organizations at various jurisdictional levels. National standards for key systems may be required to facilitate the interoperability and compatibility of major systems across jurisdictional, geographic, and functional lines.

BROAD-BASED REQUIREMENTS

Needs for new technologies, procedures, protocols, and standards to facilitate incident management are identified at both the field and the national levels. Because these needs will most likely exceed available resources, the NIMS provides a mechanism for aggregating and prioritizing them from the local to the national level. These needs will be met across the incident life-cycle by coordinating basic, applied, developmental, and demonstration research, testing, and evaluation activities.

STRATEGIC PLANNING FOR R&D

Strategic R&D planning identifies future technologies that can improve preparedness, prevention, response, and recovery capabilities or lower the cost of existing capabilities. To ensure effective R&D, the NIC, in coordination with the Under Secretary for Science and Technology of the Department of Homeland Security, will integrate into the national R&D agenda the incident management science and technology needs of departments, agencies, functional disciplines, private sector entities, and NGOs operating within the NIMS at the Federal, State, local, and Tribal levels.

SUPPORTING INCIDENT MANAGEMENT WITH SCIENCE AND TECHNOLOGY

Supporting technologies enhance incident management capabilities or lower costs through three principal activities: operational scientific support; technology standards support; and research and development support.

TECHNICAL STANDARDS SUPPORT

Technical standards support efforts enable the development and coordination of technology standards for the NIMS to ensure that personnel, organizations, communications and information systems, and other equipment perform consistently, effectively, and reliably together without disrupting one another. In coordination with the Department of Homeland Security Science and Technology Directorate, the NIC will coordinate the establishment of technical standards for NIMS users. The following principles will be used in defining these standards:

PERFORMANCE MEASUREMENTS AS A BASIS FOR STANDARDS

Performance measurement—collecting hard data on how things work in the real world—is the most reliable basis for standards that ensure the safety and mission effectiveness of emergency responders and incident managers. Within the technology standards process, a performance measurement infrastructure develops guidelines, performance standards, testing protocols, personnel certification, reassessment, and training procedures to help incident management organizations use equipment systems effectively.

CONSENSUS-BASED PERFORMANCE STANDARDS

A consensus-based approach to standards builds on existing approaches to standards for interoperable equipment and systems and takes advantage of existing SDOs with long-standing interest and expertise. These SDOs include the National Institute of Justice, National Institute for Standards and Technology, National Institute for Occupational Safety and Health, American National Standards Institute, American Society for Testing and Materials (ASTM International), and National Fire Protection Association. The NIMS, through the NIC, establishes working relationships among these SDOs and incident management organizations at all levels to develop performance standards for incident management technology.

TEST AND EVALUATION BY OBJECTIVE EXPERTS

NIMS technology criteria will rely on private- and public-sector testing laboratories to evaluate equipment against NIMS technical standards. These organizations will be selected in accordance with guidelines that ensure that testing organizations are both technically proficient and objective (free from conflicting interests) in their testing. The NIC will issue appropriate guidelines as part of its standards-development and facilitation responsibilities.

TECHNICAL GUIDELINES FOR TRAINING EMERGENCY RESPONDERS ON EQUIPMENT USE

Inputs from vulnerability analysts, equipment developers, users, and standards experts are employed to develop scientifically based technical guidelines for training emergency responders on how to use equipment properly. Based on incident management protocols, instruments, and instrument systems, these training guidelines reflect threat and vulnerability information, equipment and systems capabilities, and a range of expected operating conditions. In addition, performance measures and testing protocols developed from these training guidelines provide a reproducible method of measuring the effectiveness of equipment and systems.

RESEARCH AND DEVELOPMENT TO SOLVE OPERATIONAL PROBLEMS

R&D planning will be based on the operational needs of the entire range of NIMS users. These needs represent key inputs as the nation formulates its R&D agenda for developing new and improved incident management capabilities. Since operational needs will usually exceed the resources available for research to address them, these needs must be validated, integrated, and prioritized. The preparedness organizations described in Component I, Preparedness, Preparedness Organizations perform these functions. The Department of Homeland Security is responsible for integrating user needs at all levels into the national R&D agenda.

APPENDIX A

NATIONAL INCIDENT MANAGEMENT RESOURCE TYPING SYSTEM

PURPOSE

This appendix provides additional information regarding the national equipment typing system specified in Component III of this document.

RESPONSIBILITIES

The NIMS Integration Center (NIC) as described in Component III has the overall responsibility for ongoing development and refinement of various NIMS activities and programs. Under its auspices, the National Resource Management Working Group, chaired by the Emergency Preparedness and Response Directorate of the Department of Homeland Security, is responsible for establishing a national resource typing protocol. The NIMS resource typing protocol is based on inputs from representatives from various Federal agencies and departments and private organizations, as well as representatives of State and local emergency management; law enforcement; firefighting and emergency medical services; public health; public works; and other entities with assigned responsibilities under the Federal Response Plan and the National Response Plan. Federal, State, local, and Tribal authorities should use the national typing protocol when inventorying and managing resources to promote common interoperability and integration.

ELEMENTS OF THE NATIONAL TYPING PROTOCOL

The resource typing protocol provided by the NIMS describes resources using category, kind, components, metrics, and type data. The following data definitions will be used:

RESOURCE

For purposes of typing, resources consist of personnel, teams, facilities, supplies, and major items of equipment available for assignment to or use during incidents. Such resources may be used in tactical support or supervisory capacities at an incident site or EOC. Their descriptions include category, kind, components, metrics, and type.

CATEGORY

A category is the function for which a resource would be most useful. Table A-1 briefly describes the categories used in the national resource typing protocol.

Table A-1—Categories Used in the National Resource Typing System

CATEGORY	PURPOSE
Transportation	To assist Federal agencies, State and local governments, and voluntary organizations requiring transportation to perform incident management missions following a major disaster or emergency; to coordinate incident management operations and restoration of the transportation infrastructure
Communications	To provide communications support for Federal, State, local, and Tribal incident management efforts
Public works and engineering	To assist those engaged in lifesaving, life-sustaining, damage mitigation, and recovery operations following a major disaster or emergency by providing technical advice, evaluation, and engineering services; by contracting for construction management and inspection and for the emergency repair of water and wastewater treatment facilities; supplying potable water and ice and emergency power; and arranging for needed real estate.
Firefighting	To detect and suppress urban, suburban, and rural fires.
Information and planning	To collect, analyze, process, and disseminate information about a potential or actual disaster or emergency to facilitate overall activities in providing assistance to support planning and decision-making.

CATEGORY	PURPOSE
Law enforcement and security	To provide law enforcement assistance during response and recovery operations; to assist with site security and investigation.
Mass care	To support efforts to meet the mass care needs of disaster victims including delivering such services as supplying victims with shelter, feeding, and emergency first aid; supplying bulk distribution of emergency relief supplies; and collecting information to and for a disaster welfare information system designed to report on victim status and assist in reuniting families.
Resource management	To provide operational assistance for incident management operations.
Health and medical	To provide assistance to supplement local resources in meeting public health and medical care needs following a disaster or emergency or during a potential developing medical situation.
Search and rescue	To provide specialized lifesaving assistance in the event of a disaster or emergency, including locating, extricating, and providing on-site medical treatment to victims trapped in collapsed structures.
Hazardous materials response	To support the response to an actual or potential discharge and/or release of hazardous materials.
Food and water	To identify, secure, and arrange for the transportation of safe food and water to affected areas during a disaster or emergency.
Energy	To help restore energy systems following a disaster or emergency.
Public information	To contribute to the well-being of the community following a disaster by disseminating accurate, consistent, timely, and easy-to-understand information; to gather and disseminate information about disaster response and recovery process.
Animals and agricultural issues	To coordinate activities responding to an agricultural disaster and/or when the health or care of animals is at issue.
Volunteers and donations	To support the management of unsolicited goods and unaffiliated volunteers, and to help establish a system for managing and controlling donated goods and services.

KIND

Kind refers to broad classes that characterize like resources, such as teams, personnel, equipment, supplies, vehicles, and aircraft.

COMPONENTS

Resources can comprise multiple components. For example, an engine company may be listed as having the eight components shown in Table A-2.

Table A-2—Example of a Resource with Multiple Components (Fire Fighting Engine Company)

(1) Pump	(5) Water tank
(2) Hose 2 1/2”	(6) Ladder
(3) Hose 1 1/2”	(7) Master Stream
(4) Hose 1"	(8) Personnel

As another example, urban search and rescue (US&R) teams consist of two 31-person teams, four canines, and a comprehensive equipment cache. The cache is divided into five separate, color-coded elements and is stored in containers that meet specific requirements.

METRICS

Metrics are measurement standards. The metrics used will differ depending on the kind of resource being typed. The mission envisioned determines the specific metric selected. The metric must be useful in describing a resource’s capability to support the mission. As an example, one metric for a disaster medical assistance team is the number of patients it can care for per day. Likewise, an appropriate metric for a hose might be the number of gallons of water per hour that can flow through it. Metrics should identify capability and/or capacity.

TYPE

Type refers to the level of resource capability. Assigning the Type I label to a resource implies that it has a greater level of capability than a Type II of the same resource (for example, due to its power, size, or capacity), and so on to Type IV. Typing provides managers with additional information to aid the selection and best use of resources. In some cases, a resource may have less than or more than four types; in such cases, either additional types will be identified, or the type will be described as “not applicable.” The type assigned to a resource or a component is based on a minimum level of capability described by the identified metric(s) for that resource. For example, the U.S. Coast Guard has typed oil skimmers based on barrels per day, as outlined below in Table A-3:

Table A-3—Example of a Resource with Multiple Types (Coast Guard Oil Skimmer)

Type I 9,600 bbls/day	Type III 480 bbls/day
Type II 2,880 bbls/day	Type IV N/A

ADDITIONAL INFORMATION

The national resource typing protocol will also provide the capability to use additional information that is pertinent to resource decision-making. For example, if a particular set of resources can only be

released to support an incident under particular authorities or laws, the protocol should provide the ability for resource managers to understand such limitations.

EXAMPLE OF A RESOURCE FOR WHICH TYPING HAS BEEN COMPLETED

As an illustration of how the national equipment typing system is used, Figure A-4 is an example of a resource that has been completely typed, an urban search and rescue task force.

Table A-4—Example of a Fully Typed Resource (Urban Search and Rescue Task Forces)

Resource:	Swiftwater/Flood Search and Rescue Team					
Category:	Search and Rescue			Kind:	Team	
Minimum Capabilities:		Type I	Type II	Type III	Type IV	Other
Component	Metric					
Personnel	Team Composition	14 member team 2 managers 2 squad leaders 10 personnel	6 member team 1 squad leader 5 personnel	4 member team 1 squad leader 3 personnel	3 member team 1 squad leader 2 personnel	
Personnel	Minimum number Technical Animal Rescue	2	1	1		
Personnel	Minimum number ALS Certified	2				
Personnel	Minimum number Helicopter/ Aquatic Rescue Operations	4	2			
Personnel	Minimum number Powered Boat Operators	4	2			

Resource:	Swiftwater/Flood Search and Rescue Team					
Category:	Search and Rescue			Kind:	Team	
Minimum Capabilities:		Type I	Type II	Type III	Type IV	Other
Component	Metric					
Personnel	Minimum number SCUBA Trained Support Personnel with Equipment	4	2	2		
Personnel	Number and level EMTs	14 EMT - B 2 EMT - P	Same as Type III	Same as Type IV	1 EMT - B	
Team	Sustained operations	Same as Type II	24-hour operations	Same as Type IV	18-hour operations	
Team	Capabilities	Manage search operations Power vessel operations Helicopter rescue operational Animal rescue HazMat ALS Communications Logistics	Manage search operations Power vessel operations Helicopter rescue operational Animal rescue HazMat BLS	Assist in search operations Nonpowered water craft Animal rescue HazMat BLS	Low-risk operations Land-based HazMat BLS	
Team	Specialty S&R Capabilities	Same as Type II	Same as Type III plus: Technical rope systems	In-water contact rescue Dive rescue		
Team	Training	Same as Type II except: Divers to have 80 hours of formal public safety diver training	Same as Type III plus: Helicopter operations Awareness Technical rope rescue	Same as Type IV plus: Divers to have 60 hours of formal public safety diver training	Class 3 paddle skills Contact and self-rescue skills HazMat ICS Swiftwater rescue technician	

Resource:	Swiftwater/Flood Search and Rescue Team					
Category:	Search and Rescue			Kind:	Team	
Minimum Capabilities:		Type I	Type II	Type III	Type IV	Other
Component	Metric					
Team	Certifications	ALS Advanced First Aid & CPR	Same as Type IV	Same as Type IV	BLS Advanced First Aid & CPR	
Equipment	Transportation Resources	Equipment trailer; Personnel support vehicle				
Equipment	Communication	Same as Type II	Same as Type III plus: Aircraft radio	Same as Type IV plus: Headset	Batteries Portable radios Cell phone	
Equipment	Medical	ALS medical kit Blankets Spineboard Litter	Same as Type III plus: Spineboard	Same as Type IV plus: Litter	BLS medical kit Blankets	
Equipment	Personal	Same as Type II	Same as Type III: plus: Life vests HEED except: PFD Type V	Same as Type IV plus: Fins Lamps	Flares; Markers; Bags; Flashlight; Gloves; Helmets; Light sticks; PFD Type III/IV; Knives; Shoes; Whistles	
Equipment	SCUBA	Same as Type III	Same as Type III	SCUBA cylinder Buoyancy compensator Weight belt 2 cutting tools Chest harness & snap shackle Full face mask U/W communication Dry suit Search line Spare SCUBA		

Resource:	Swiftwater/Flood Search and Rescue Team					
Category:	Search and Rescue			Kind:	Team	
Minimum Capabilities:		Type I	Type II	Type III	Type IV	Other
Component	Metric					
				cylinder		
Vehicle	Rescue Boat	2 - Fueled	1 - Fueled	1 - Non-powered 4 person		
Comments:	Conduct search and rescue operations in all water environments including swiftwater and flood conditions. Water rescue teams come with all team equipment required to safely and effectively conduct operations. For a complete listing of recommended training, skills, and equipment, please reference the FIRESCOPE Swiftwater/Flood Search and Rescue definition at: http://www.firescope.org/ics-usar/ICS-SF-SAR-020-1.pdf.					

APPENDIX B

INCIDENT COMMAND SYSTEM

The Incident Command System (ICS) is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in incident management activities. It is used for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade, including catastrophic acts of terrorism. ICS is used by all levels of government—Federal, State, local, and Tribal, as well as by many private sector and nongovernmental organizations. ICS is usually organized around five major functional areas: command, operations, planning, logistics, and finance and administration. A sixth functional area, Intelligence, may be established if deemed necessary by the Incident Commander, depending on the requirements of the situation at hand.

More up-to-date and detailed information, regarding ICS—and other examples of ICS application, can be found through the NIC website: http://www.fema.gov/emergency/nims/nims.shtm.

Some of the more important "transitional steps" that are necessary to apply ICS in a field incident environment include the following:

- recognizing and anticipating the requirement that organizational elements will be activated and taking the necessary steps to delegate authority as appropriate;
- establishing incident facilities as needed, strategically located, to support field operations;
- establishing the use of common terminology for organizational functional elements, position titles, facilities, and resources; and
- rapidly evolving from providing oral direction to the development of a written Incident Action Plan.

TAB 1—ICS ORGANIZATION

FUNCTIONAL STRUCTURE

The ICS organization comprises five major functional areas (Figure B-1): command, operations, planning, logistics, and finance and administration.[42] (A sixth area, intelligence, may be established if required.)

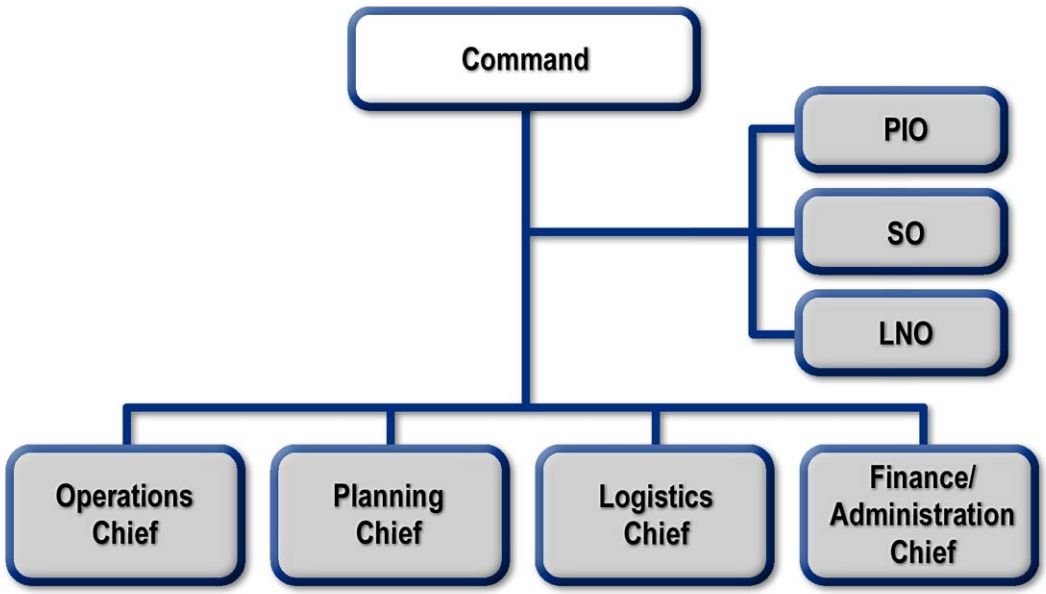


Figure B-1—Incident Command System: Basic Functional Structure

[42] Summary information on the major components of ICS is contained in Appendix C.

MODULAR EXTENSION

The ICS organizational structure is modular, extending to incorporate all elements necessary for the type, size, scope, and complexity of a given incident. The IC structural organization builds from the top down; responsibility and performance begin with the incident command element and the IC. When the need arises, four separate sections can be used to organize the staff. Each of these may have several subordinate units, or Branches, depending on the management requirements of the incident. If one individual can simultaneously manage all major functional areas, no further organization is required. If one or more of the functions requires independent management, an individual is assigned responsibility for that function.

The initial responding IC may determine that it is necessary to delegate functional management to one or more Section Chiefs in order to maintain a manageable span of control. However, the IC will typically establish task forces or strike teams under a division or group supervisor or branch director for operational management. When two or more Branches are established for operations, the IC may designate an Operations Section Chief and other appropriate Section Chiefs. The Section Chiefs will further delegate management authority for their areas as required. If a Section Chief sees the need, he or she may establish Branches or units (depending on the section). Similarly, each functional unit leader will further assign individual tasks within the unit as needed.

The use of deputies and assistants is a vital part of both the ICS organizational structure and the modular concept. The Incident Commander may have one or more deputies, whom may be from the same agency, or from an assisting agency. Deputies may also be used at section and branch levels of the ICS organization. The only ICS requirement regarding the use of a deputy, whether at the Incident Commander, Section, or Branch level, is that the deputy must be fully qualified to assume the position.

There are three primary reasons to designate a deputy Incident Commander:

1. To perform specific tasks as requested by the Incident Commander.

2. To perform the incident command function in a relief capacity, e.g., to take over the next operational period. (In this case the deputy will assume the primary role.)

3. To represent an assisting agency that may share jurisdiction or have jurisdiction in the future.

Assistants are used as subordinates for the Command Staff positions, particularly Information Officer and Safety Officer. They have a level of technical capability, qualifications, and responsibility subordinate to primary positions. Assistants may also be used at camps to supervise unit activities (e.g, Assistant Ground Support Unit Leader, Camp #2).

The modular concept described above is based on the following considerations:

- developing the form of the organization to match the function or task to be performed;
- staffing only the functional elements that are required to perform the task;
- observing recommended span-of-control guidelines;

- performing the function of any non-activated organizational element at the next highest level; and
- deactivating organizational elements no longer required.

For reference, Table B-1 describes the distinctive title assigned to each element of the ICS organization at each corresponding level, as well as the leadership title corresponding to each individual element.

Table B-1—ICS Organization

ORGANIZATIONAL ELEMENT	LEADERSHIP POSITION TITLES	SUPPORT POSITIONS
Incident Command	Incident Commander (IC)	Deputy
Command Staff	Officer	Assistant
Section	Section Chief	Deputy
Branch	Branch Director	Deputy
Divisions and Groups*	Supervisors	N/A
Unit**	Unit Leader	Manager, Coordinator
Strike Team/Task Force	Leader	Single Resource Boss, Companies/Crews
Single Resource Boss	Boss	N/A
Technical Specialist	Specialist	N/A

*The hierarchical term *supervisor* is only used in the Operations Section.

****Unit leader designations apply to the subunits of the Operations, Planning, Logistics, and Finance/Administration Sections.**

COMMAND STAFF

In an incident command organization, the Command Staff consists of Incident Command and various special staff positions. The special staff positions are specifically designated, report directly to Incident Command, and are assigned responsibility for key activities that are not a part of the ICS General Staff functional elements. Three special staff positions are typically identified in ICS: (1) Public Information Officer, (2) Safety Officer, and (3) Liaison Officer. Additional positions may be required, depending on the nature, scope, complexity, and location(s) of the incident(s), or according to specific requirements established by the IC.

PUBLIC INFORMATION OFFICER

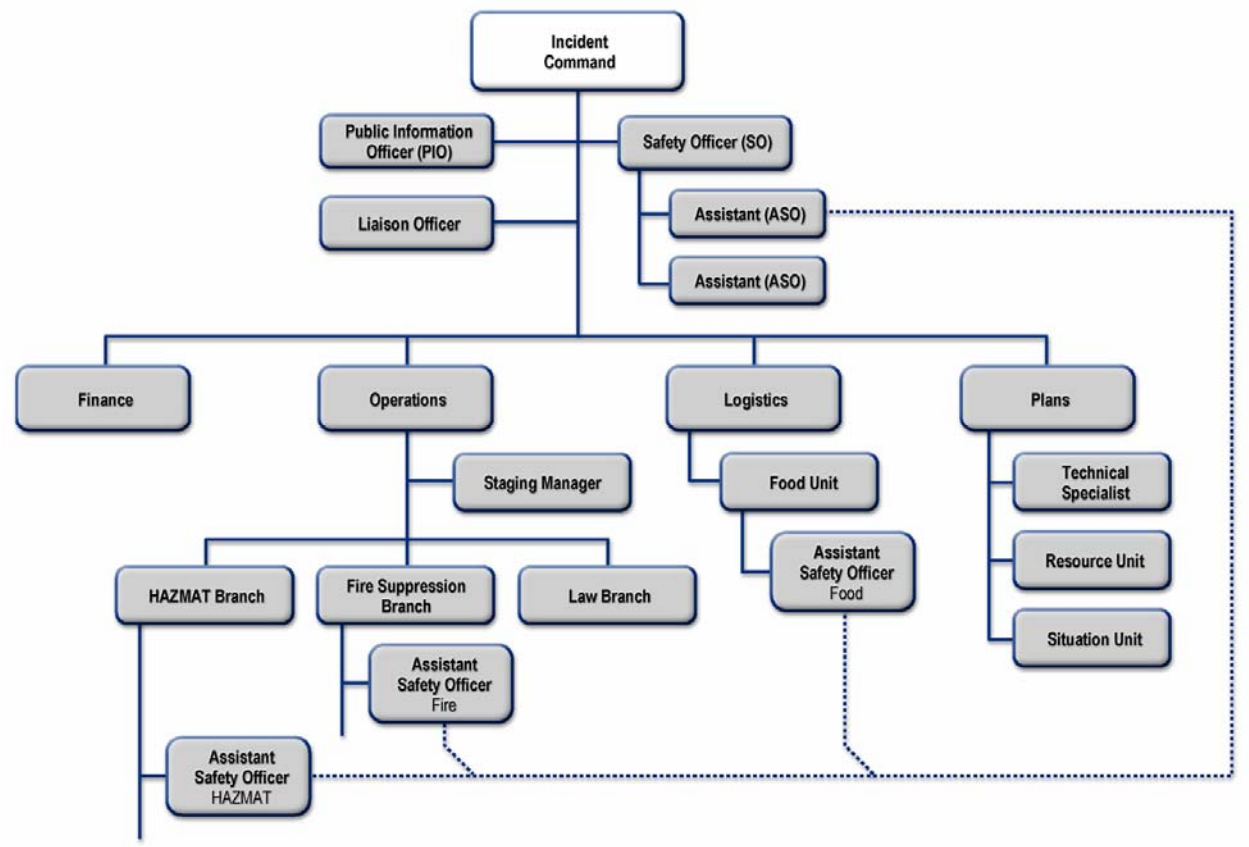
The PIO is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements. The PIO develops accurate and complete information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external consumption. The PIO may also perform a key public information-monitoring role. Whether the command structure is single or unified, only one incident PIO should be

designated. Assistants may be assigned from other agencies or departments involved. The IC must approve the release of all incident-related information.

SAFETY OFFICER

The SO monitors incident operations and advises Incident Command on all matters relating to operational safety, including the health and safety of emergency responder personnel. The ultimate responsibility for the safe conduct of incident management operations rests with the IC or UC and supervisors at all levels of incident management. The SO is, in turn, responsible to Incident Command for the set of systems and procedures necessary to ensure ongoing assessment of hazardous environments, coordination of multi-agency safety efforts, and implementation of measures to promote emergency responder safety, as well as the general safety of incident operations. The SO has emergency authority to stop and/or prevent unsafe acts during incident operations. In a UC structure, a single SO should be designated regardless of the involvement of multiple jurisdictions and/or functional agencies. The SO, Operations Section Chief, and Planning Section Chief must coordinate closely regarding operational safety and emergency responder health and safety issues. The SO must also ensure the coordination of safety management functions and issues across jurisdictions, across functional agencies, and with the private sector and NGOs. It is important to note that the agencies, organizations, or jurisdictions that contribute to joint safety management efforts do not lose their individual identities or responsibility for their own programs, policies, and personnel. Rather, each entity contributes to the overall effort to protect all responder personnel involved in incident operations.

Assistant Safety Officers may be required and may be assigned from other agencies or departments constituting the UC. Some types of incident such as a hazardous materials incident require assistant safety officers to have special skill sets. Figure B-2 is an illustrative example of a how the Safety Officer and the respective Assistant Safety Officers are positioned in an incident.



*The dotted line connection is meant to show coordination between the two points, not a direct link within the chain of command.

Figure B-2—Illustrative Example of the Role of ASO in ICS in a Multi-Branch Incident

- The assistant safety officer for HAZMAT would be assigned to carry out the functions outlined in 29-CR-1910.120 (HAZMAT Operations). This person would have the required knowledge, skills and abilities to provide oversight for specific hazardous material operations at field level.
- The assistant safety officer fire would be assigned to assist the branch director providing oversight for specific fire operations. This person should have the required knowledge, skills and abilities to provide this function.
- The assistant safety officer food would be assigned to the food unit to provide oversight of the food handling and distribution. This person should have the required knowledge, skills and abilities to provide this function. An example would be a food specialist from a local health department.

LIAISON OFFICER

The LNO is Incident Command's point of contact for representatives of other governmental agencies, NGOs, and/or private entities (with no jurisdiction or legal authority), to provide input on their agency's policies, resource availability, and other incident related matters. In either a single IC or UC structure, representatives from assisting or cooperating agencies and organizations coordinate through the LNO. Agency and/or organizational representatives assigned to an incident must have the authority to speak for their parent agencies and/or organizations on all matters, following appropriate consultations with their agency leadership. Assistants and personnel from other agencies or organizations (public or private) involved in incident management activities may be assigned to the LNO to facilitate coordination.

ADDITIONAL COMMAND STAFF

Additional Command Staff positions may also be necessary depending on the nature and location(s) of the incident, and/or specific requirements established by Incident Command. For example, a Legal Counsel may be assigned to Plans section as a technical specialist or directly to the Command Staff to advise Incident Command on legal matters, such as emergency proclamations, legality of evacuation orders, and legal rights and restrictions pertaining to media access. Similarly, a Medical Advisor may be designated and assigned directly to the Command Staff to provide advice and recommendations to Incident Command in the context of incidents involving medical and mental health services, mass casualty, acute care, vector control, epidemiology, and/or mass prophylaxis considerations, particularly in the response to a bioterrorism incident.

TAB 2—THE OPERATIONS SECTION

The Operations Section is responsible for managing tactical operations at the incident site directed toward reducing the immediate hazard, saving lives and property, establishing situation control, and restoring normal conditions. Incidents can include acts of terrorism, wildland and urban fires, floods, hazardous material spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other incidents requiring an emergency response.

Because of its functional unit management structure, the ICS is applicable across a spectrum of incidents differing in size, scope, and complexity. The types of agencies that could be included in the Operations Section include fire, law enforcement, public health, public works, and emergency services, working together as a unit or in combinations, depending on the situation. Many incidents may involve private individuals, companies, or nongovernmental organizations, some of which may be fully trained and qualified to participate as partners in the Operations Section.

Incident operations can be organized and executed in many ways. The specific method selected will depend on the type of incident, agencies involved, and objectives and strategies of the incident management effort. The following discussion presents several different methods of organizing incident tactical operations. In some cases, a method will be selected to accommodate jurisdictional boundaries. In other cases, the approach will be strictly functional. In still others, a mix of functional and geographical approaches may be appropriate. While ICS organizational management is always established in a top-down manner, it is driven by the number of subordinate units or single resources. This is in order to maintain a manageable span of control for all resources. The ICS offers extensive flexibility in determining the appropriate approach using the factors described above. Figure B-3 shows the primary organizational structure within the Operations Section.

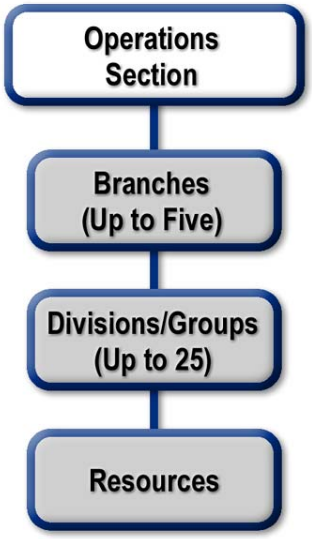


Figure B-3—Major Organizational Elements of Incident Operations

OPERATIONS SECTION CHIEF

The Operations Section Chief directly manages all incident tactical activities and implements the IAP. The Operations Section Chief may have one or more deputies (preferably from other agencies in multi-jurisdictional incidents). Deputies will be qualified to a similar level as the Operations Section Chief. An Operations Section Chief should be designated for each operational period and will have direct involvement in the preparation of the IAP for the period of responsibility.

BRANCHES

Branches may be established to serve several purposes including the following:

THE NUMBERS OF DIVISIONS AND/OR GROUPS EXCEED THE RECOMMENDED SPAN OF CONTROL FOR THE OPERATIONS SECTION CHIEF

The recommended span of control for the Operations Section Chief (as for all managers and supervisory personnel) is 1:5. When this ratio is exceeded, the Operations Section Chief may set up Branches to provide more direct supervision for individual resources. If the number of individual resources continues to grow, the Branch Directors may establish Divisions and/or Groups to maintain the desired span of control (see Figure B-4). For example, if one group and four divisions are reporting to the Operations Section Chief, and two divisions and one group are to be added, a two-branch organization may be formed.

Within ICS, the span of control of any individual with incident management supervisory responsibility should range from three to seven subordinates, with the optimum being five. The type of incident, nature of the task, hazards and safety factors, and distances between personnel and resources all influence span-of-control considerations.

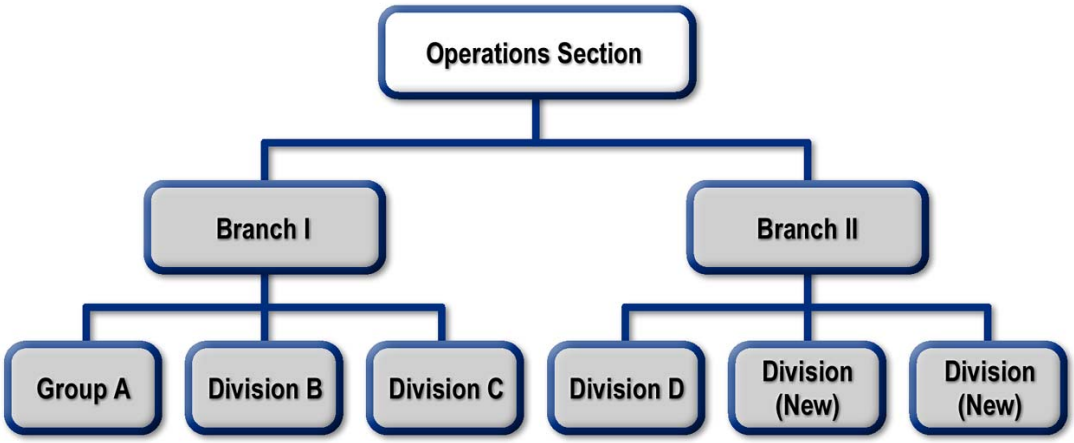


Figure B-4—Geographic Branch Organization

THE NATURE OF THE INCIDENT CALLS FOR A FUNCTIONAL BRANCH STRUCTURE

For example, if a large aircraft crashes within a city, various departments within the city (including police, fire, emergency services, and public health services) would each have a functional branch operating under the direction of a single Operations Section Chief. In this example (see Figure B-5, the Operations Section Chief is from the fire department, with deputies from police and EMS services. Other alignments could be made, depending on the city plan and type of emergency. Note that, in this

situation, the Incident Command could be either a single command or Unified Command (UC), depending on the jurisdiction.

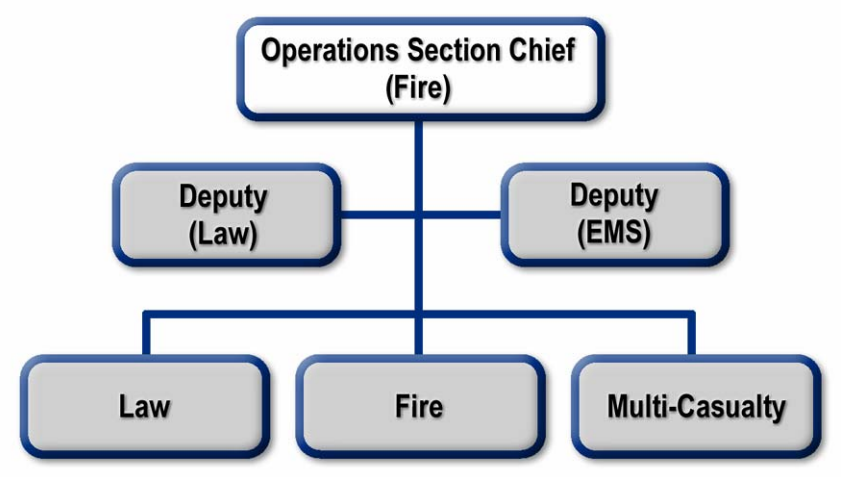


Figure B-5—Functional Branch Structure

THE NATURE OF THE INCIDENT CALLS FOR A MULTIJURISDICTIONAL BRANCH STRUCTURE

In this case, resources are best managed under the agencies that normally control them (see Figure B-6). For example, the response to a major flood might require combining Federal, State, county, city, and Tribal resources. Figure B-7 shows an illustrative example of Law Enforcement's on scene response in an ICS structure.

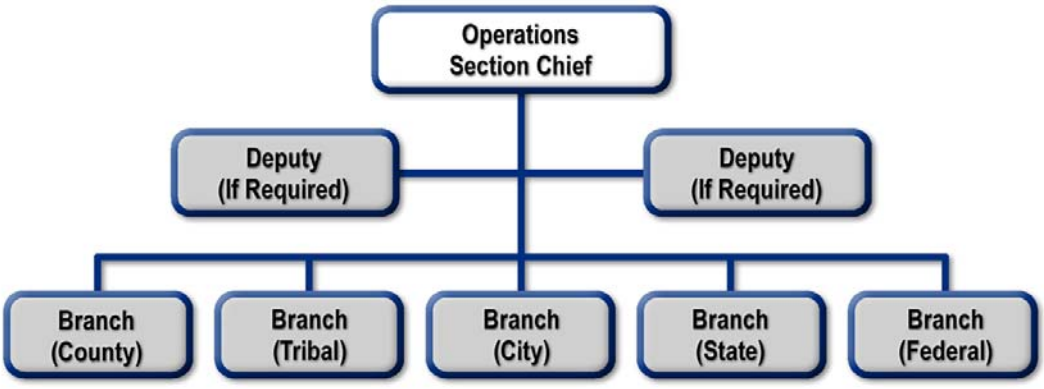


Figure B-6—Multi-jurisdictional Incident

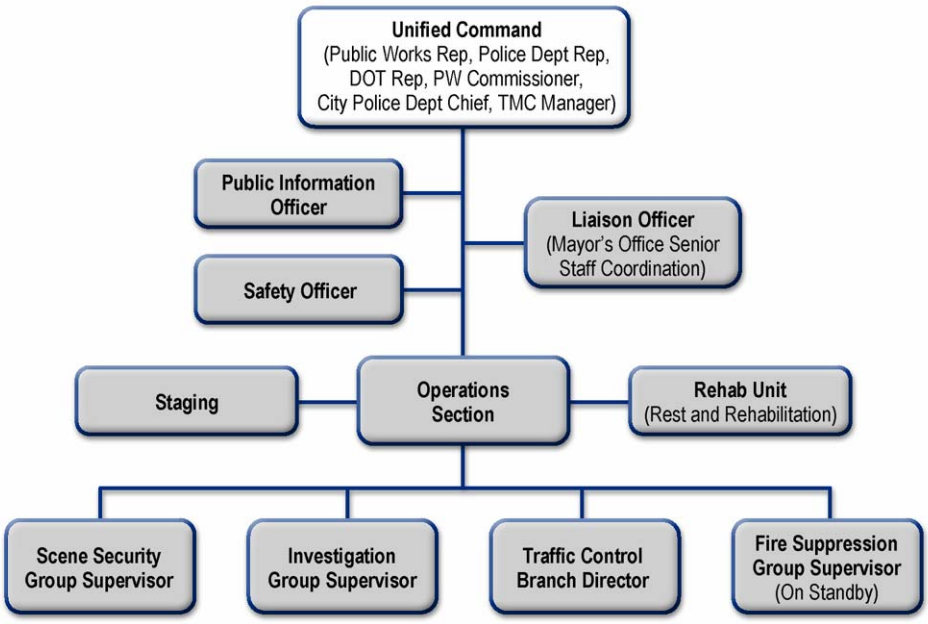


Figure B-7—Illustrative Example of a Law Enforcement Response under a Unified Command

DIVISIONS AND GROUPS

Divisions and groups are established when the number of resources exceeds the Operations Section Chief's manageable span of control. Divisions demarcate physical or geographical areas of operation within the incident area. Groups demarcate functional areas of operation for the incident.

The use of the two terms is necessary, because *division* always refers to a geographical assignment and *group* always refers to a functional assignment. Both divisions and groups may be used in a single incident if there is justification for their use and if proper coordination can be effected.

As additional types of resources are added to the organization, resources should be assigned into a division structure.

GEOGRAPHICAL DIVISIONS

The best way to create geographical divisions is to divide an area according to natural separations of terrain or other prominent geographical features, such as rivers. When geographical features are used for determining boundaries, the size of the division should correspond to appropriate span-of-control guidelines. See Figure B-8.

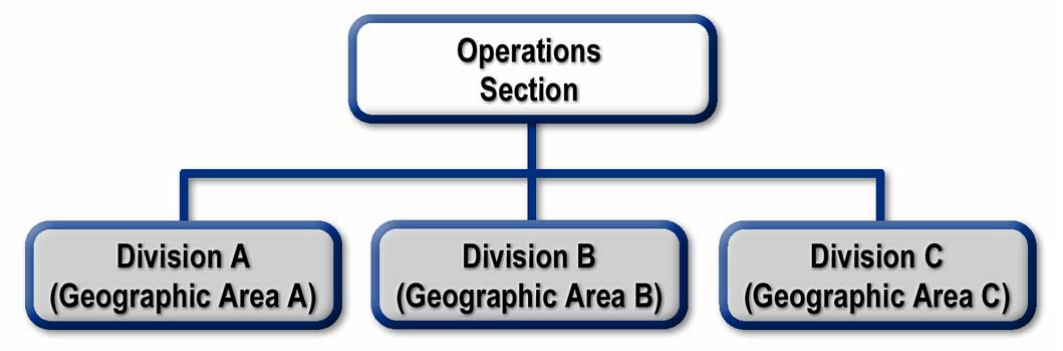


Figure B-8—Use of Geographical Divisions

FUNCTIONAL GROUPS

Functional groups can best be used to describe areas of like activity (e.g., rescue, evacuation, medical). See Figure B-9.

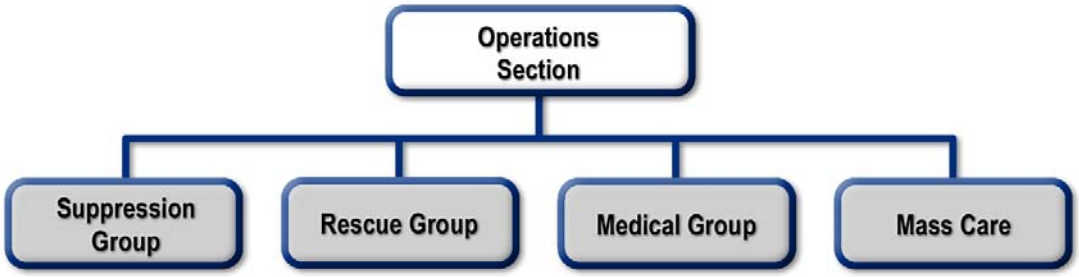


Figure B-9—Use of Functional Groups

COMBINED GEOGRAPHICAL DIVISIONS AND FUNCTIONAL GROUPS

It is also possible to have both divisions and groups within the Operations Section. For example, Divisions A, B, and C (based on geographical locations) may work in conjunction with functional groups

assigned to specific tasks (e.g. traffic control, smoke ventilation, etc.) in those locations. Alternatively, group designations may be made for the entire incident and will work in conjunction with all divisions assigned to the Operations Section. Organizationally, the supervisors of Divisions and Groups have the same level of authority.

RESOURCE ORGANIZATION

Initially, in any incident, individual resources that are assigned will report directly to the IC. As the incident grows in size or complexity, individual resources may be organized and employed in a number of ways to facilitate incident management:

SINGLE RESOURCES

Resources may be employed on an individual basis. This is typically the case in the context of the initial response to the incident. During sustained operations, situations will typically arise that call for the use of a single helicopter, vehicle, mobile equipment, etc.

TASK FORCES

Task Forces are any combination of resources put together to accomplish a specific mission. Task Forces have a designated leader and operate with common communications. Combining resources into Task Forces allows several key resource elements to be managed under one individual's supervision, thus aiding in span of control. In many instances, the initial response resources will be organized in a "task force" configuration with different units/resources working together under a common leadership (e.g. police, fire, and EMS respond to a motor vehicle accident). This can be used as a building block for establishing supervision for additional resources that may be needed.

STRIKE TEAMS

A Strike Team consists of a set number of resources of the same kind and type operating under a designated leader with common communications between them. Strike Teams represent known capability and are highly effective management units.

AIR OPERATIONS BRANCH

The Operations Section Chief may establish an Air Operations Branch to meet mission requirements in certain situations, in which size, organization, and operation will depend primarily on the nature of the incident and the availability of air assets.[43] Figure B-10 shows a typical organizational structure for air operations.

The Operations Section Chief may designate a director for the Air Operations Branch when the complexity of air operations requires additional support and effort or when the incident requires mixing tactical and logistical utilization of helicopters and other aircraft. Flight safety is a paramount concern in complex operations and supports the requirement for a designated Air Operations Branch to ensure the deconfliction of assets and the integration of safety considerations into operational planning and mission execution.

Whenever both helicopters and fixed-wing aircraft must operate simultaneously within the incident air space, an Air Tactical Group Supervisor should be designated. This individual coordinates all airborne activity with the assistance of a helicopter coordinator and a fixed-wing coordinator. When only one helicopter is used, however, the helicopter may be directly under the control of the Operations Section Chief.

The Air Support Group establishes and operates bases for rotary-wing air assets and maintains required liaison with off-incident fixed-wing bases. The Air Support Group is responsible for all timekeeping for aviation assets assigned to the incident.

[43] Air Operations Branch is used here as an example and may not be applicable to all ICS organizations.

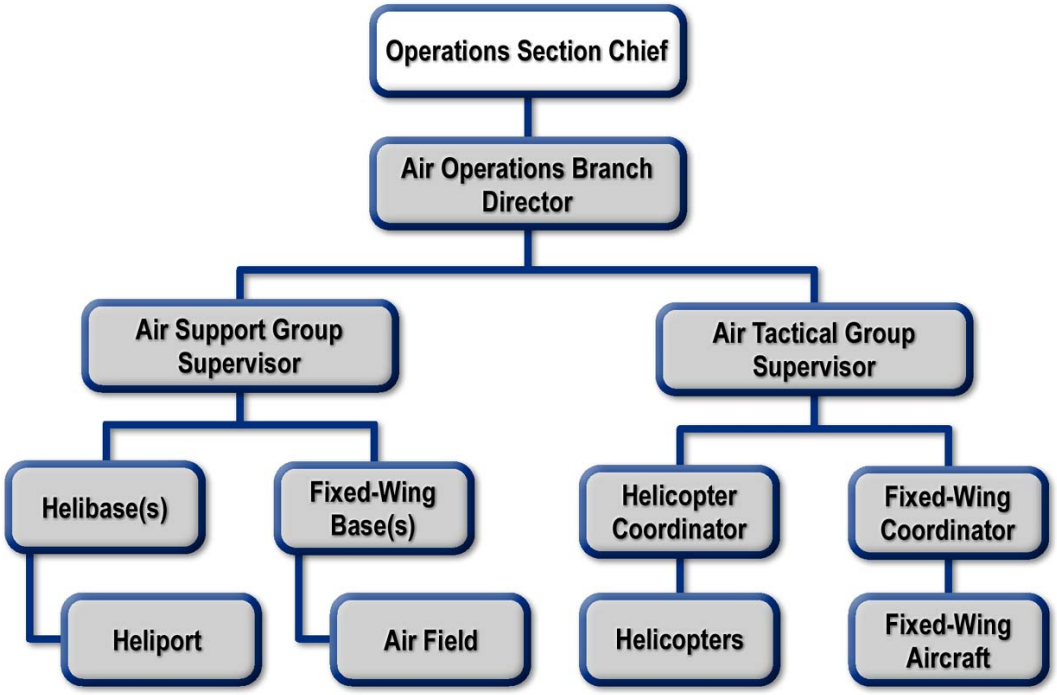


Figure B-10—Air Operations Organization

TAB 3—THE PLANNING SECTION

The Planning Section is responsible for collecting, evaluating, and disseminating tactical information pertaining to the incident. This section maintains information and intelligence on the current and forecasted situation, as well as the status of resources assigned to the incident. The Planning Section prepares and documents IAPs and incident maps and gathers and disseminates information and intelligence critical to the incident. As shown in Figure B-11, the Planning Section has four primary units and may also include technical specialists to assist in evaluating the situation and forecasting requirements for additional personnel and equipment.

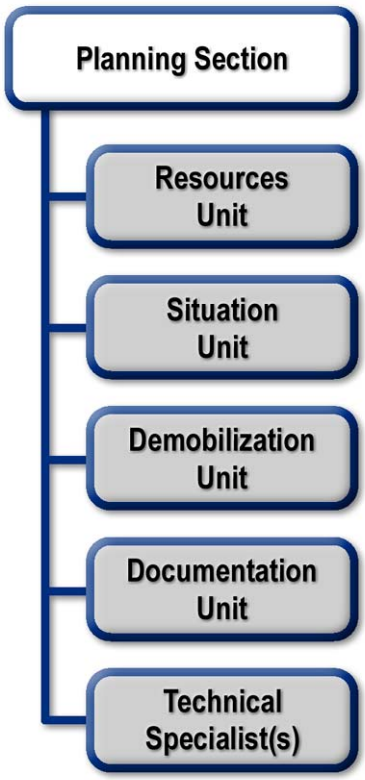


Figure B-11—Planning Section Organization

PLANNING SECTION CHIEF

The Planning Section Chief (PSC) oversees all incident-related data gathering and analysis regarding incident operations and assigned resources, develops alternatives for tactical operations, conducts planning meetings, and prepares the IAP for each operational period. This individual will normally come from the jurisdiction with primary incident responsibility and may have one or more deputies from other participating jurisdictions.

RESOURCES UNIT

RESPONSIBILITIES

Physical resources consist of personnel, teams, facilities, supplies, and major items of equipment available for assignment to or employment during incidents. The Resources Unit makes certain that all assigned personnel and other resources have checked in at the incident. This unit maintains a system for keeping track of the current location and status of all assigned resources and maintains a master list of all resources committed to incident operations.

MANAGING RESOURCES

For effective management of their employment, resources must be categorized by capability and capacity across disciplines and tracked continuously as to status. The following tools are necessary for maintaining an up-to-date and accurate picture of resource utilization:

STATUS CONDITIONS

Tactical resources at an incident can have one of three status conditions:

- **Assigned resources:** are personnel, teams, equipment, or facilities that have checked in (or in the case of equipment and facilities, receipted for) and are supporting incident operations.
- **Available resources:** are personnel, teams, equipment, or facilities that have been assigned to an incident and are ready for a specific work detail or function.

- **Out-of-service resources:** are personnel, teams, equipment, or facilities that have been assigned to an incident but are unable to function for mechanical, rest, or personal reasons; or because their condition makes them unusable.

CHANGES IN STATUS

Typically, when the status of a resource has changed (e.g. a unit that was previously listed as "out-of-service" is reclassified as "available"), the Unit Leader of the supervisor who approved the status change should immediately notify the Resource Unit Leader who, in turn, will make the appropriate status classifications.

SITUATION UNIT

The Situation Unit collects, processes, and organizes ongoing situation information; prepares situation summaries; and develops projections and forecasts of future events related to the incident. The Situation Unit also prepares maps and gathers and disseminates information and intelligence for use in the IAP and is prepared to provide situation reports in a timely manner at the request of the PSC or IC. This unit may also require the expertise of technical specialists and operations and information security specialists.

DOCUMENTATION UNIT

The Documentation Unit maintains accurate and complete incident files, including a complete record of the major steps taken to resolve the incident; provides duplication services to incident personnel; and files, maintains, and stores incident files for legal, analytical, and historical purposes. Documentation is part of the Planning Section primarily because this unit prepares the IAP and maintains the files and records that are developed as part of the overall IAP and planning function.

DEMOBILIZATION UNIT

The Demobilization Unit develops an Incident Demobilization Plan that includes specific instructions for all personnel and resources that will require demobilization. This unit should begin its work early in the incident, creating rosters of personnel and resources and obtaining any missing information as check-in proceeds.

Note that many city- and county-provided resources, because they are local, do not require specific demobilization instructions. Once the Incident Demobilization Plan has been approved, the Demobilization Unit ensures that it is distributed both at the incident and elsewhere as necessary.

TECHNICAL SPECIALISTS

The ICS is designed to function in a wide variety of incident scenarios requiring the use of technical specialists. These personnel have special skills and are activated only when needed. Specialists may serve anywhere within the organization, including the Command Staff. No minimum qualifications are prescribed, as technical specialists normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically specially certified in their fields or professions.

Technical specialists assigned to the Planning Section may report directly to its chief, may report to any function in an existing unit, or may form a separate unit within the Planning Section, depending on the requirements of the incident and the needs of the Section Chief. Technical specialists may also be assigned to other parts of the organization (e.g., to the Operations Section to assist with tactical matters or to the Finance/Administration Section to assist with fiscal matters). For example, a legal specialist or legal counsel may be assigned directly to the Command Staff to advise the IC on legal matters, such as emergency proclamations, legality of evacuation orders, and legal rights and restrictions pertaining to media access. Generally, if the expertise is needed for only a short period and normally involves only one individual, that individual should be assigned to the Situation Unit. If the expertise will be required on a long-term basis and may require several personnel, it is advisable to establish a separate Technical Unit in the Planning Section.

The incident itself will primarily dictate the needs for technical specialists. Below are representative examples of the kinds of specialists that may be required:

- meteorologist
- environmental impact specialist
- resource use and cost specialists

- flood control specialist
- water-use specialist
- explosives specialist
- structural engineering specialist
- firefighter specialist
- medical and/or public health specialist
- medical intelligence specialist
- pharmaceutical specialist
- veterinarian
- agricultural specialist
- toxicologist
- radiation health physicist
- intelligence specialist
- infectious disease specialist
- chemical or radiological decontamination specialist
- law enforcement specialist
- legal counsel
- industrial hygienist
- transportation specialist
- scientific support coordinator
- mass care specialist
- numerical modeler
- data management specialist.

A specific example of the need to establish a distinct technical unit within the General Staff is the requirement to coordinate and manage large volumes of environmental sampling and/or analytical data from multiple sources in the context of certain complex incidents, particularly those involving biological, chemical, and radiation hazards. To meet this requirement, an Environmental Unit could be established within the Planning Section to facilitate interagency environmental data management, monitoring, sampling, analysis, and assessment. The Environmental Unit would prepare environmental data for the situation unit and work in close coordination with other units and sections within the ICS

structure to enable effective decision support to the IC or UC. Technical specialists assigned to the Environmental Unit might include a scientific support coordinator and sampling, response technologies, weather forecast, resources at risk, cleanup assessment, and disposal technical specialists. Example tasks accomplished by the Environmental Unit would include the following:

- identifying sensitive areas and recommending response priorities;
- developing a plan for collecting, transporting, and analyzing samples;
- providing input on wildlife protection strategies;
- determining the extent and effects of site contamination;
- developing site cleanup and hazardous material disposal plans; and
- identifying the need for and obtaining permits and other authorizations.

TAB 4—THE LOGISTICS SECTION

The Logistics Section meets all support needs for the incident, including ordering resources through appropriate procurement authorities from off-incident locations. It also provides facilities, transportation, supplies, equipment maintenance and fueling, food service, communications, and medical services for incident personnel. See Figure B-17.

The Logistics Section is led by a Section Chief, who may also have a deputy. Having a deputy is encouraged when all designated units are established at an incident site. When the incident is very large or requires a number of facilities with large numbers of equipment, the Logistics Section can be divided into two Branches. This helps with span of control by providing more effective supervision and coordination among the individual units. Conversely, in smaller incidents or when fewer resources are needed, a Branch configuration may be used to combine the task assignments of individual units with a Branch structure. (Figure B-12 provides an example of the Logistics Section with individual units, Figure B-13 provides an example of how Branches may be established to supervise/coordinate units or perform their tasks.)

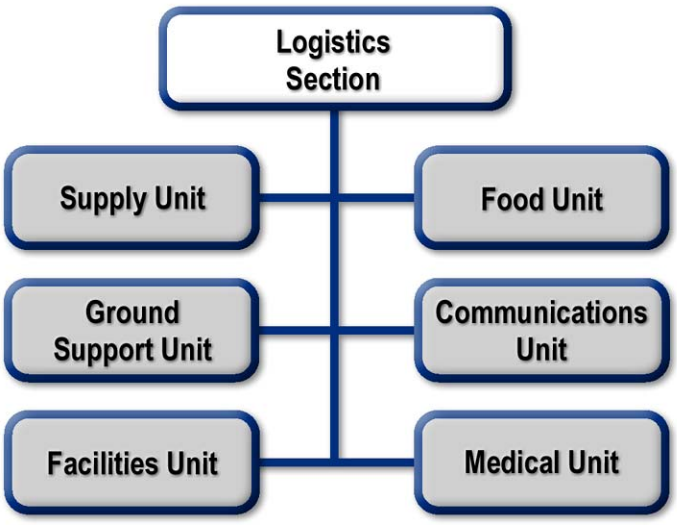


Figure B-12—Logistics Section Organization

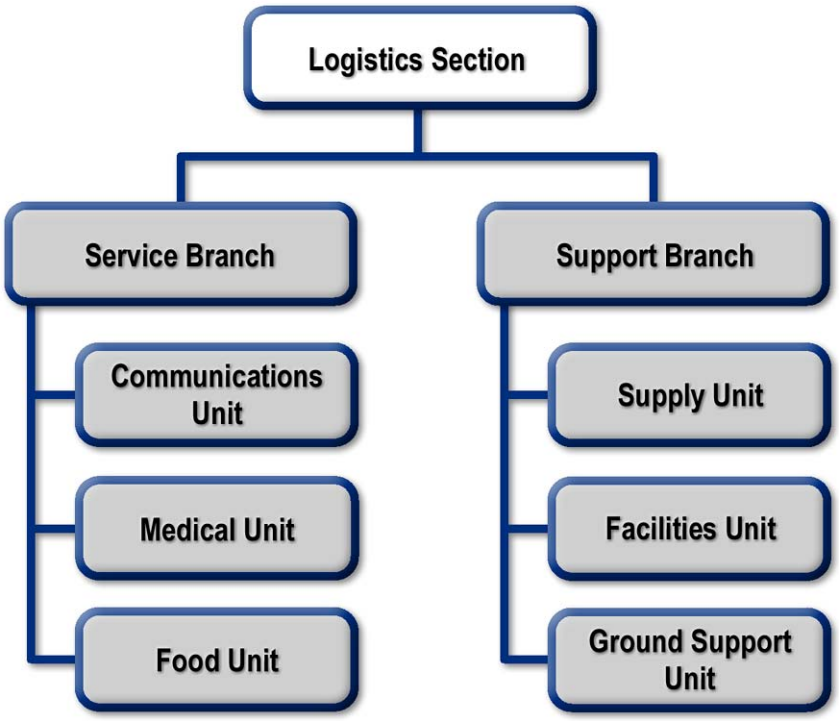


Figure B-13—Logistics Section: Two-Branch Organizational Structure

SUPPLY UNIT

The Supply Unit orders, receives, stores, and processes all incident-related resources, personnel, and supplies.

Once established, the Supply Unit also has the basic responsibility for all off-incident ordering, including:

- all tactical and support resources (including personnel); and
- all expendable and nonexpendable supplies required for incident support.

The Supply Unit provides the support required to receive, process, store, and distribute all supply orders. The unit also handles tool operations, which include storing, disbursing, and servicing of all

tools and portable, nonexpendable equipment. Additionally, the Supply Unit assists in projecting resource needs based upon information provided from the IAP.

FACILITIES UNIT

The Facilities Unit sets up, maintains, and demobilizes all facilities used in support of incident operations. The unit also provides facility maintenance and security services required to support incident operations.

The Facilities Unit sets up the ICP, incident base, and camps (including trailers and/or other forms of shelter for use in and around the incident area), as well as sanitary facilities, food service areas, etc. The incident base and camps may often be established in areas having existing structures, which may be used in their entirety or only in part. The Facilities Unit also provides and sets up necessary personnel support facilities, including areas for

- food and water service;
- sleeping;
- sanitation and showers; and
- staging.

This unit also orders, through supply, such additional support items as portable toilets, shower facilities, and lighting units.

Note that providing shelter for victims is a critical operational activity, which will be incorporated into the IAP. Sheltering will normally be conducted by appropriate nongovernmental organization staff, such as the American Red Cross or other similar entities.

GROUND SUPPORT UNIT

The Ground Support Unit

- maintains and repairs primary tactical vehicles, and mobile ground support equipment;

- records usage time for all ground equipment (including contract equipment) assigned to the incident;
- supplies fuel for all mobile equipment;
- provides transportation in support of incident operations (except aircraft); and
- develops and implements the Incident Traffic Plan.

In addition to its primary functions of maintaining and servicing vehicles and mobile equipment, the Ground Support Unit also maintains a transportation pool for major incidents. This pool consists of vehicles (e.g., staff cars, buses, pick-ups) that are suitable for transporting personnel. The Ground Support Unit also provides up-to-date information on the location and status of transportation vehicles to the Resources Unit.

COMMUNICATIONS UNIT

The Communications Unit develops the Communications Plan (ICS205) to make the most effective use of the communications equipment and facilities assigned to the incident, installs and tests all communications equipment, supervises and operates the incident communications center, distributes and recovers communications equipment assigned to incident personnel, and maintains and repairs communications equipment on site.

The Communications Unit's major responsibility is effective communications planning for the ICS, especially in the context of a multi-agency incident. This is critical for determining required radio nets, establishing interagency frequency assignments, and ensuring the interoperability and the optimal use of all assigned communications capabilities.

The Communications Unit Leader should attend all incident-planning meetings to ensure that the communication systems available for the incident can support tactical operations planned for the next operational period.

Incident communications are managed through the use of a common communications plan and an incident-based communications center established solely for the use of tactical and support resources assigned to the incident.

Advance planning is required to ensure that an appropriate communications system is available to support incident operations requirements. This planning includes the development of frequency inventories, frequency-use agreements, and interagency radio caches.

Most complex incidents will require an Incident Communications Plan. The Communications Unit is responsible for planning the use of radio frequencies; establishing networks for command, tactical,

support, and air units; setting up on-site telephone and public address equipment; and providing any required off-incident communication links. Codes should not be used for radio communication; a clear spoken message—based on common terminology that avoids misunderstanding in complex and noisy situations—reduces the chances for error.

Radio networks for large incidents will normally be organized as follows:

COMMAND NET

The Command Net links together: incident command, command staff, section chiefs, branch directors, division, and group supervisors.

TACTICAL NETS

Several tactical nets may be established to connect agencies, departments, geographical areas, or specific functional units. The determination of how nets are set up should be a joint planning, operations, and logistics function. The Communications Unit Leader will develop the overall plan.

SUPPORT NET

A support net may be established primarily to handle changes in resource status but also to handle logistical requests and other non-tactical functions.

GROUND-TO-AIR NET

To coordinate ground-to-air traffic, either a specific tactical frequency may be designated, or regular tactical nets may be used.

AIR-TO-AIR NETS

Air-to-air nets will normally be pre-designated and assigned for use at the incident.

FOOD UNIT

Note: Feeding affected persons (e.g. victims, evacuees, persons at shelters, etc.) is a critical operational activity, which will normally be incorporated into the IAP. Feeding activities will normally be conducted by members of appropriate NGOs, such as the American Red Cross or similar entities. Services provided by appropriate NGOs would not fall within the Food Unit but in a separate functional assignment which should be communicated and coordinated with the IC and Operations Section Chief to ensure operational continuity.

The Food Unit determines food and water requirements; plans menus, orders food, provides cooking facilities, cooks, serves, maintains food service areas, and manages food security and safety concerns.

Efficient food service is important, but especially so for any extended incident. The Food Unit must be able to anticipate incident needs, both in terms of the number of people who will need to be fed and whether the type, location, or complexity of the incident indicates that there may be special food requirements. The unit must supply food needs for the entire incident, including all remote locations (e.g. camps and staging areas), as well as supply food service to operations personnel unable leave operational assignments. The Food Unit must interact closely with the following elements:

- Planning Section, to determine the number personnel that must be fed;
- Facilities Unit, to arrange food-service areas;
- Supply Unit, to order food, unless provided under contract or agreement;
- Ground Support Unit, to obtain ground transportation; and
- Air Operations Branch Director, to obtain air transportation.

Careful planning and monitoring is required to ensure food safety before and during food service operations, including the assignment, as indicated, of public health professionals with expertise in environmental health and food safety.

MEDICAL UNIT

Note: Patient care and medical services for those who are not incident personnel (e.g. victims of a bioterror attack, hurricane victims, etc.) are critical operational activities associated with a host of potential incident scenarios. As such, these activities are incorporated into the IAP as key considerations of the Plans and Operations Sections. These sections should be staffed accordingly with appropriately qualified Emergency Medical Services, public health, medical personnel, technical experts, and other professional personnel, as required.

The primary responsibilities of the Medical Unit include the following:

- develop the Incident Medical Plan (*for incident personnel*);

- develop procedures for handling any major medical emergency involving incident personnel;
- provide continuity of medical care, including vaccinations, vector control, occupational health, prophylaxis, and mental health services for incident personnel;
- provide transportation for injured incident personnel;
- coordinate, established, and/or staff routine rest and rehabilitation of incident responders;
- ensure that incident personnel patients are tracked as they move from origin, to care facility, to final disposition;
- assist in processing all paperwork related to injuries or deaths of incident assigned personnel; and
- coordinate personnel and mortuary affairs for incident personnel fatalities.

The Medical Unit is responsible for the effective and efficient provision of medical services to incident personnel, and reports directly to the Logistics Section Chief. The Medical Unit Leader will develop a medical plan, which will, in turn, form part of the IAP. The medical plan should provide specific information on medical assistance capabilities at incident locations, potential hazardous areas or conditions, and off-incident medical assistance facilities and procedures for handling complex medical emergencies. The Medical Unit will also assist the Finance/Administration Section with the administrative requirements related to injury compensation, including obtaining written authorizations, billing forms, witness statements, administrative medical documents, and reimbursement as required. The Medical Unit will ensure patient privacy to the fullest extent possible.

TAB 5—THE FINANCE/ ADMINISTRATION SECTION

When there is a specific need for financial, reimbursement (individual and agency or department), and/or administrative services to support incident management activities, a Finance/Administration Section is established. Under the ICS, not all agencies will require such assistance. In large, complex scenarios involving significant funding originating from multiple sources, the Finance/Administrative Section is an essential part of the ICS. In addition to monitoring multiple sources of funds, the Section Chief must track and report to the IC the financial "burn rate" as the incident progresses. This allows the IC to forecast the need for additional funds before operations are affected negatively. This is particularly important if significant operational assets are under contract from the private sector. The Section Chief may also need to monitor cost expenditures to ensure that statutory rules that apply are met. Close coordination with the Planning Section and Logistics Section is also essential so that operational records can be reconciled with financial documents. Note that, in some cases, only one specific function may be required (e.g., cost analysis), which a technical specialist in the Planning Section could provide. Figure B-14 illustrates the basic Finance/Administration Section organizational structure.

While the functions of Finance and Administration are critical components of effective command and management, in some incidents, components of the Finance/Administration section may not be staffed on-scene. Modern (wireless) communications systems enable the Finance/Administration functions to be performed remotely from the incident scene, typically in the normal work stations where these functions would customarily be performed.

The Finance/Administration Section Chief will determine, given current and anticipated future requirements, the need for establishing specific subordinate units. In some of the functional areas (e.g., procurement), an actual unit need not be established if it would consist of only one person. In such a case, a procurement technical specialist would be assigned in the Planning Section instead. Because of the specialized nature of finance functions, the Section Chief should come from the agency that has the greatest requirement for this support. The Section Chief may have a deputy.

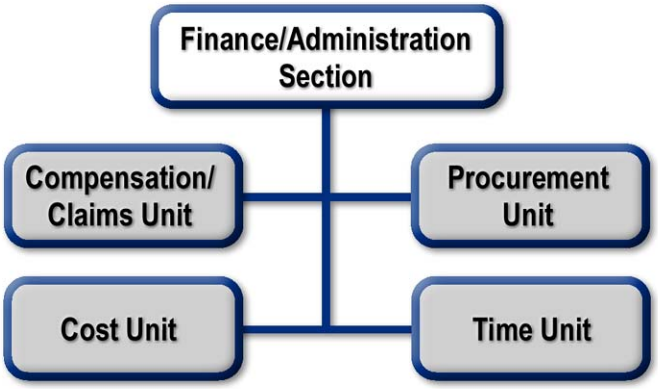


Figure B-14—Finance and Administration Section Organization

TIME UNIT

The Time Unit is primarily responsible for ensuring proper daily recording of personnel time, in accordance with the policies of the relevant agencies. The Time Unit also ensures that the Logistics Section records or captures equipment usage time, through the Ground Support Unit for ground equipment and through the Air Operations Support Group for aircraft.

If applicable (depending on the agencies involved), personnel time records will be collected and processed for each operational period. The unit leader may require the assistance of personnel familiar with the relevant policies of any affected agencies. These records must be verified, checked for accuracy, and posted according to existing policies. Excess hours worked must also be determined, for which separate logs must be maintained.

PROCUREMENT UNIT

The Procurement Unit administers all financial matters pertaining to vendor contracts. This unit coordinates with local jurisdictions to identify sources for equipment, prepares and signs equipment

rental agreements, and processes all administrative requirements associated with equipment rental and supply contracts.

Note that, in some agencies, the Supply Unit in the Logistics Section will be responsible for certain procurement activities. The Procurement Unit will also work closely with local cost authorities.

COMPENSATION AND CLAIMS UNIT

Under ICS, a single unit handles injury compensation and claims. The specific activities are, of course, varied and may not always be accomplished by the same person. The individual handling injury compensation ensures that all forms required by workers' compensation programs and local agencies are completed. This individual also maintains files on injuries and illnesses associated with the incident and ensures that all witness statements are obtained in writing. Since the Medical Unit may also perform certain of these tasks, close coordination between the Medical and Compensation and Claims Units is essential. The claims function handles investigations of all civil tort claims involving property associated with or involved in the incident. The Compensation and Claims Unit maintains logs on the claims, obtains witness statements, and documents investigations and agency follow-up requirements.

COST UNIT

The Cost Unit provides cost analysis data for the incident. This unit must ensure that equipment and personnel for which payment is required are properly identified, obtain and record all cost data, and analyze and prepare estimates of incident costs. The Cost Unit also provides input on cost estimates for resource use to the Planning Section. The Cost Unit must maintain accurate information on the actual costs of all assigned resources.

TAB 6—ESTABLISHING AN AREA COMMAND

An Area Command is established when the complexity of the incident and incident management span-of-control considerations so dictate. Generally, the administrator(s) of the agency having jurisdictional responsibility for the incident makes the decision to establish an Area Command.

The purpose of an Area Command is either to oversee the management of multiple incidents that are each being handled by a separate ICS organization or to oversee the management of a very large or complex incident that has multiple incident management teams engaged.

This type of command is generally used when there are a number of incidents in the same area and of the same type, such as two or more HAZMAT spills or fires. These are usually the kinds of incidents that may compete for the same resources. When incidents are of different types and/or do not have similar resource demands, they are usually handled as separate incidents or are coordinated through an EOC. If the incidents under the authority of the Area Command span multiple jurisdictions, a Unified Area Command should be established. This allows each jurisdiction involved to have appropriate representation in the Area Command.

Area Commands are particularly relevant to public health emergencies, given that these incidents are typically not site specific, not immediately identifiable, geographically dispersed, and evolve over time ranging from days to weeks. Such incidents as these, as well as acts of biological, chemical, radiological, and nuclear terrorism, call for a coordinated intergovernmental, private sector, and nongovernmental organization response, with large-scale coordination typically conducted at a higher jurisdictional level.

RESPONSIBILITIES

The Area Command does not have operational responsibilities. For the incidents under its authority, the Area Command:

- sets overall agency incident-related priorities;
- allocates critical resources according to the established priorities;
- ensures that incidents are properly managed;

- ensures effective communications;
- ensures that incident management objectives are met and do not conflict with each other or with agency policies;
- identifies critical resource needs and reports them to the established multi-agency coordination system entities;
- ensures that short-term "emergency" recovery is coordinated to assist in the transition to full recovery operations; and
- provides for personnel accountability and a safe operating environment.

The Area Command develops an action plan detailing incident management priorities, needs, and objectives. This plan should clearly state policy, objectives, and priorities; provide a structural organization with clear lines of authority and communications; and identify incident management functions to be performed by the Area Command (i.e., public communications).

ORGANIZATION

The Area Command organization operates under the same basic principles as ICS. Typically, an Area Command will comprise the following key personnel, all of whom must possess appropriate qualifications and certifications:

AREA COMMANDER (UNIFIED AREA COMMAND)

The Area Commander is responsible for the overall direction of the incident management teams assigned to the same incident or to incidents in close proximity. This responsibility includes ensuring that conflicts are resolved, that incident objectives are established, and that strategies are selected for the use of critical resources. The Area Command is also responsible for coordinating with Federal, State, local, Tribal, and participating private organizations.

ASSISTANT AREA COMMANDER—LOGISTICS

The Area Command Logistics Chief provides facilities, services, and materials at the Area Command level and ensures the effective allocation of critical resources and supplies among the incident management teams.

ASSISTANT AREA COMMANDER—PLANNING

The Area Command Planning Chief collects information from various incident management teams to assess and evaluate potential conflicts in establishing incident objectives, strategies, and priorities for allocating critical resources.

AREA COMMAND SUPPORT POSITIONS

The following positions are activated as necessary.

AREA COMMAND CRITICAL RESOURCES UNIT LEADER

The critical resources unit leader tracks and maintains the status and availability of critical resources assigned to each incident under the Area Command—Planning.

AREA COMMAND PATIENT TRANSPORTATION COORDINATOR

The Patient Transportation Coordinator coordinates the movement of patients to prevent the overloading of hospitals.

AREA COMMAND SITUATION UNIT LEADER

The situation unit leader monitors the status of objectives for each incident or IMT assigned to the Area Command—Planning.

AREA COMMAND PUBLIC INFORMATION OFFICER

The PIO provides public information coordination between incident locations and serves as the point of contact for media requests to the Area Command. Specifically the Public Information Officer also:

AREA COMMAND LIAISON OFFICER

The liaison officer helps maintain off-incident interagency contacts and coordination.

AREA COMMAND AVIATION COORDINATOR

An aviation coordinator is assigned when aviation resources are competing for common airspace and critical resources, and works in coordination with incident aviation organizations to evaluate potential conflicts, develop common airspace management procedures, and prioritize critical resources.

AREA COMMAND MOBILIZATION MANAGER

The Area Command Mobilization Manager maintains accountability of available area command resources prior to allocation. Assigned to the Assistant Area Command—Logistics.

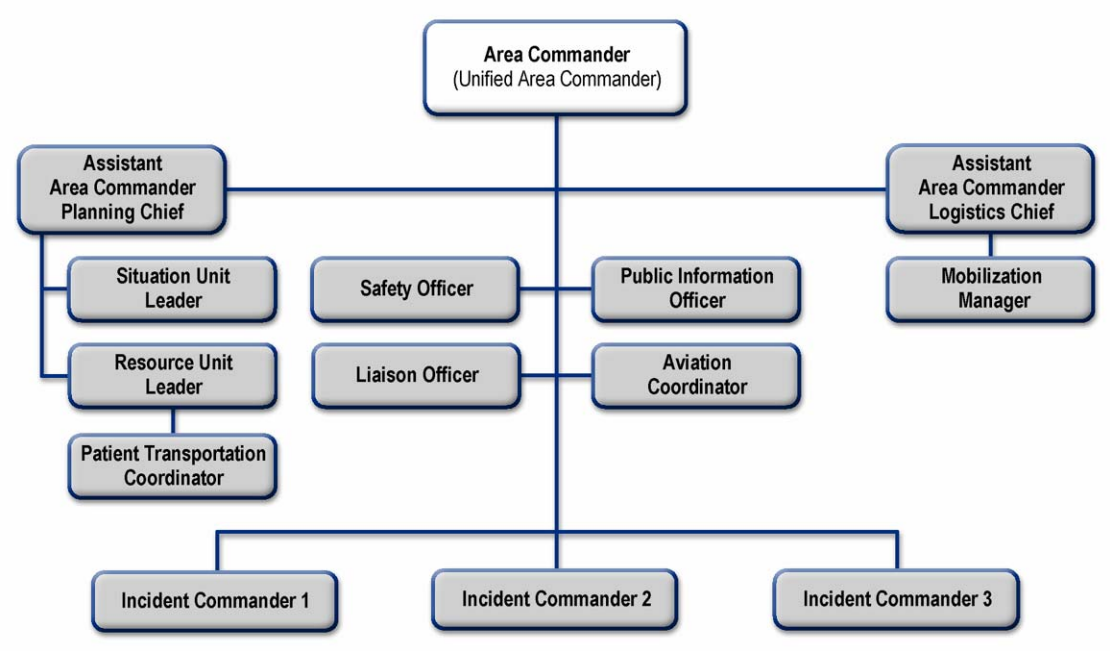


Figure B-15— Illustrative Example of Area Command in a Multi-Casualty Incident

LOCATION

The following guidelines should be followed in locating an Area Command:

- To the extent possible, the area command should be established in close proximity to the incidents under its authority. This makes it easier for the Area Commander and the ICs to meet and otherwise interact.
- It is, however, best not to co-locate an Area Command with any individual ICP. Doing so might cause confusion with the command and management activities associated with that particular incident.
- Area commands must establish effective, efficient communications and coordination processes and protocols with subordinate ICPs, as well as with other incident management organizations involved in incident operations.
- The facility used to house the organization should be large enough to accommodate a full Area Command staff. It should also be able to accommodate meetings between the Area Command staff, the ICs, and agency executive(s), as well as news media representatives.
- Area Commands may be co-located with EOCs.

REPORTING RELATIONSHIPS

When an Area Command is involved in coordinating multiple incident management activities, the following reporting relationships will apply:

- The ICs for the incidents under the Area Command's authority report to the Area Commander.
- The Area Commander is accountable to the agency(s) or to the jurisdictional executive(s) or administrator(s).
- If one or more incidents within the Area Command are multi-jurisdictional, a Unified Area Command should be established. In this instance, ICs would report to the Unified Area Commander for their jurisdiction.

TAB 7—PREDESIGNATED FACILITIES AND LOCATIONS

Several kinds and types of facilities may be established in and around the incident area. The requirements of the incident and the desires of the IC will determine the specific kinds of facilities used and their locations and may consist of the following designated facilities, among various others:

INCIDENT COMMAND POST

The ICP signifies the location of the tactical-level, on-scene incident command and management organization. It typically comprises the IC and immediate staff and may include other designated incident management officials and responders from Federal, State, local, and Tribal agencies, as well as private sector and nongovernmental organizations. Typically, the ICP is located at or in the immediate vicinity of the incident site and is the locus for the conduct of direct, on-scene control of tactical operations. Incident planning is also conducted at the ICP; an incident communications center also would normally be established at this location. The ICP may be co-located with the incident base, if the communications requirements can be met. The ICP may perform local EOC-like functions in the context of smaller jurisdictions or less complex incident scenarios.

INCIDENT BASE

An Incident Base is the location at which primary support activities are conducted. A single incident base is established to house all equipment and personnel support operations. The Logistics Section,

which orders all resources and supplies, is also located at this base. The Incident Base should be designed to be able to support operations at multiple incident sites.

CAMPS

Camps are separate from the Incident Base and are located in satellite fashion from the Incident Base where they can best support incident operations. Camps provide certain essential auxiliary forms of support, such as food, sleeping areas, and sanitation. Camps may also provide minor maintenance and servicing of equipment. Camps may be relocated to meet changing operational requirements.

MOBILIZATION AND STAGING AREAS

Staging areas are established for temporary location of available resources. Staging Areas will be established by the Operations Section Chief to enable positioning of and accounting for resources not immediately assigned. A Staging Area can be any location in which personnel, supplies, and equipment can be temporarily housed or parked while awaiting operational assignment. Staging Areas may include temporary feeding, fueling, and sanitation services. The Operations Section Chief assigns a manager for each Staging Area, who checks in all incoming resources, dispatches resources at the Operations Section Chief's request, and requests Logistics Section Support, as necessary, for resources located in the Staging Area. Personnel check in with the Staging Area Manager or the Resources Unit at the Staging Area, while supplies and equipment are checked in with the Supply Unit. If neither of these functions is activated, resources report to the Staging Area Manager for direction. An Area Command Staging Manager may be assigned to maintain accountability of available area command resources prior to allocation.

TAB 8—THE PLANNING PROCESS

OVERVIEW

Sound, timely planning provides the foundation for effective incident management. The NIMS planning process described below represents a template for strategic, operational, and tactical planning that includes all steps an IC and other members of the Command and General Staffs should take to develop and disseminate an Incident Action Plan (IAP). The planning process may begin with the scheduling of a planned event, the identification of a credible threat, or with the initial response to an actual or impending event. The process continues with the implementation of the formalized steps and staffing required to develop a written IAP.

A clear, concise IAP template is essential to guide the initial incident management decision process and the continuing collective planning activities of incident management teams. The planning process should provide the following:

- current information that accurately describes the incident situation and resource status;
- predictions of the probable course of events;
- alternative strategies to attain critical incident objectives; and
- an accurate, realistic, IAP for the next operational period.

Five primary phases must be followed, in sequence, to ensure a comprehensive IAP. These phases are designed to enable the accomplishment of incident objectives within a specified time. The IAP must provide clear strategic direction and include a comprehensive listing of the tactical objectives, resources, reserves, and support required to accomplish each overarching incident objective. The comprehensive IAP will state the sequence of events in a coordinated way for achieving multiple incident objectives. However, the IAP is a living document prepared based on the best available information at the time of the planning meeting. Planning meetings should not be delayed in anticipation of future information.

The primary phases of the planning process are essentially the same for the IC who develops the initial plan, for the IC and Operations Section Chief revising the initial plan for extended operations, and for

the incident management team developing a formal IAP, each following a similar process. During the initial stages of incident management, planners must develop a simple plan that can be communicated through concise oral briefings. Frequently, this plan must be developed very quickly and with incomplete situation information. As the incident management effort evolves over time, additional lead-time, staff, information systems, and technologies enable more detailed planning and cataloging of events and "lessons learned."

The five primary phases in the planning process are: (1) Understand the Situation, (2) Establish Incident Objectives and Strategy, (3) Develop the Plan, (4) Prepare and Disseminate the Plan, and (5) Evaluate and Revise the Plan.

UNDERSTAND THE SITUATION

The first phase includes gathering, recording, analyzing, and displaying situation and resource information in a manner that will ensure

- a clear picture of the magnitude, complexity, and potential impact of the incident; and
- the ability to determine the resources required to develop and implement an effective IAP.

ESTABLISH INCIDENT OBJECTIVES AND STRATEGY

The second phase includes formulating and prioritizing measurable incident objectives and identifying an appropriate strategy. The incident objectives and strategy must conform to the legal obligations and management objectives of all affected agencies.

Reasonable alternative strategies that will accomplish overall incident objectives are identified, analyzed, and evaluated to determine the most appropriate strategy for the situation at hand. Evaluation criteria include public health and safety factors; estimated costs; and various environmental, legal, and political considerations.

DEVELOP THE PLAN

The third phase involves determining the tactical direction and the specific resource, reserves, and support requirements for implementing the selected strategy for one operational period. This phase is usually the responsibility of the IC, who bases decisions on resources allocated to enable a sustained response. After determining the availability of resources, the IC develops a plan that makes the best use of these resources.

Prior to the formal planning meetings, each member of the Command Staff and each functional Section Chief is responsible for gathering certain information to support these decisions. During the Planning Meeting, the Section Chiefs develop the plan collectively.

PREPARE AND DISSEMINATE THE PLAN

The fourth phase involves preparing the plan in a format that is appropriate for the level of complexity of the incident. For the initial response, the format is a well-prepared outline for an oral briefing. For most incidents that will span multiple operational periods, the plan will be developed in writing according to ICS procedures.

EVALUATE AND REVISE THE PLAN

The planning process includes the requirement to evaluate planned events and check the accuracy of information to be used in planning for subsequent operational periods. The General Staff should regularly compare planned progress with actual progress. When deviations occur and when new information emerges, that information should be included in the first step of the process used for modifying the current plan or developing the plan for the subsequent operational period.

RESPONSIBILITIES AND SPECIFIC PLANNING ACTIVITIES

The following is a checklist of planning responsibilities and specific planning activities:

GENERAL RESPONSIBILITIES

The general responsibilities associated with the Planning Meeting and the development of the IAP are described below. The Planning Section Chief should review these with the General Staff prior to the planning meeting.

PLANNING SECTION CHIEF

- Conduct the Planning Meeting and coordinate preparation of the IAP.

INCIDENT COMMANDER

- Provide overall control objectives and strategy.
- Establish procedures for off-incident resource ordering.
- Establish procedures for resource activation, mobilization, and employment.
- Approve completed IAP plan by signature.

FINANCE SECTION CHIEF

- Provide cost implications of control objectives, as required.
- Evaluate facilities being used to determine if any special arrangements are needed.
- Ensure that the IAP is within the financial limits established by the IC.

OPERATIONS SECTION CHIEF

- Determine division work assignments and resource requirements.

LOGISTICS SECTION CHIEF

- Ensure that incident facilities are adequate.
- Ensure that the resource ordering procedure is made known to appropriate agency dispatch center(s).
- Develop a transportation system to support operational needs.
- Ensure that the section can logistically support the IAP.
- Place order(s) for resources.

OPERATIONAL PERIOD PLANNING CYCLE

The following is a graphical representation of the planning cycle as denoted by the Coast Guard Field Operations Guide.

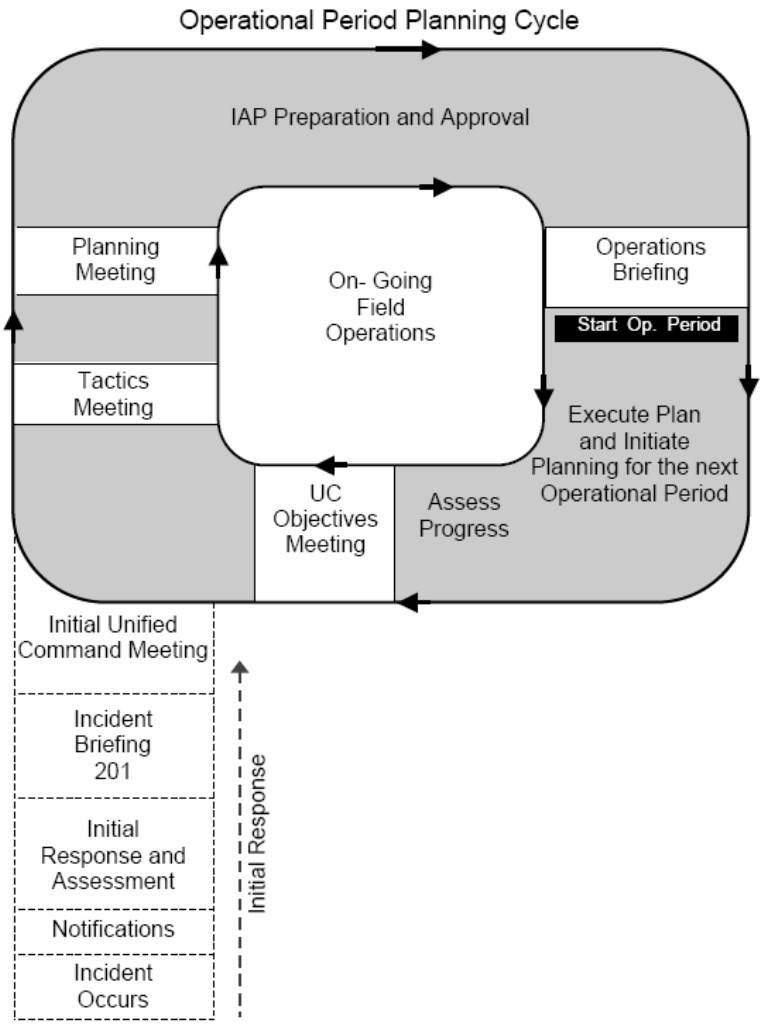


Figure B-16—Operational Period Planning Cycle

APPENDIX B

PREPLANNING STEPS: UNDERSTANDING THE PROBLEM AND ESTABLISHING OBJECTIVES AND STRATEGY

The Planning Section Chief should take the following actions prior to the initial Planning Meeting (if possible, obtaining a completed Incident Briefing Form ICS 201):

- Evaluate the current situation and decide whether the current planning is adequate for the remainder of the operational period (i.e., until next plan takes effect).
- Advise the IC and the Operations Section Chief of any suggested revisions to the current plan, as necessary.
- Establish a planning cycle for the IC.
- Determine Planning Meeting attendees in consultation with the IC. For major incidents, attendees should include
  - Incident Commander
  - Command Staff members
  - General Staff members
  - Resources Unit Leader
  - Situation Unit Leader
  - Air Operations Branch Director (if established)
  - Communications Unit Leader
  - Technical and/or Specialists (as required)
  - Agency representatives (as required).
- Establish the location and time for the Planning Meeting.
- Ensure that planning boards and forms are available.
- Notify necessary support staff about the meeting and their assignments.
- Ensure that a current situation and resource briefing will be available for the meeting.
- Obtain an estimate of regional resource availability from agency dispatch for use in planning for the next operational period.
- Obtain necessary agency policy, legal, or fiscal constraints for use in the Planning Meeting.

CONDUCTING THE PLANNING MEETING

The Planning Meeting is normally conducted by the Planning Section Chief. The checklist that follows is intended to provide a basic sequence of steps to aid the Planning Section Chief in developing the IAP. The planning checklist is used with the ICS Planning Matrix Board and/or ICS Form 215—*Operational Planning Worksheet*.[44] (The worksheet is laid out in the same manner as the Planning Matrix Board.) Every incident must have an action plan. However, not all incidents require written plans. The need for written plans and attachments is based on the requirements of the incident and the decision of the IC.

The Planning Meeting checklist is as follows:

- give briefing on situation and resource status (Planning Section)
- set control objectives (IC)
- plot control lines and division boundaries (Operations Section)
- specify tactics for each Division or Group (Operations Section)
- specify resources needed by Division or Group (Operations Section, Planning Section)
- specify facilities and reporting locations plot on map (Operations Section, Planning Section, Logistics Section)
- place resource and overhead personnel order (Logistics Section)
- consider communications, medical, and traffic plan requirements (Planning Section, Logistics Section)
- finalize, approve, and implement IAP (IC, Planning Section, Operations Section).

BRIEF ON SITUATION AND RESOURCE STATUS

The Planning Section Chief and/or Resources and Situation Unit Leaders should provide an up-to-date briefing on the situation. Information for this briefing may come from any or all of the following sources:

- Initial Incident Commander
- Incident Briefing Form (ICS 201)
- field observations
- operations reports

[44] For examples of ICS Forms, see Appendix B, Tab 9.

- regional resources and situation reports.

SET CONTROL OBJECTIVES

This step is accomplished by the IC. The control objectives are not limited to any single operational period but will consider the total incident situation. The IC will establish the general strategy to be used; will state any major policy, legal, or fiscal constraints on accomplishing the objectives; and will offer appropriate contingency considerations.

PLOT CONTROL LINES AND DIVISION BOUNDARIES ON MAP

This step is normally accomplished by the Operations Section Chief (for the next operational period) in conjunction with the Planning Section Chief who will determine control line locations, establish division and branch boundaries for geographical divisions, and determine the need for functional group assignments for the next operational period. These will be plotted on the map.

SPECIFY TACTICS FOR EACH DIVISION

After determining division geographical assignments, the Operations Section Chief will establish the specific work assignments to be used for each division for the next operational period. (Note that it may be necessary or desirable to establish a functional group in addition to geographical divisions.) Tactics (work assignments) must be specific and must be within the boundaries set by the IC's general control objectives (strategies). These work assignments should be recorded on the planning matrix. The IC, Operations Section Chief, and Logistics Section Chief should also at this time consider the need for any alternative strategies or tactics and ensure that these are properly noted on the planning matrix.

SPECIFY RESOURCES NEEDED BY DIVISION

After specifying tactics for each division, the Operations Section Chief, in conjunction with the Planning Section Chief, will determine the resource needs by division to accomplish the work assignments. Resource needs will be recorded on the planning matrix. Resource needs should be considered on basis of the type of resources required to accomplish the assignment.

SPECIFY OPERATIONS FACILITIES AND REPORTING LOCATIONS AND PLOT ON MAP

The Operations Section Chief, in conjunction with the Planning and Logistics Section Chiefs, should designate and make available the facilities and reporting locations required to accomplish Operations Section work assignments. The Operations Section Chief should also at this time indicate the reporting time requirements for the resources and any special resource assignments.

PLACE RESOURCE AND PERSONNEL ORDER

At this time, the Planning Section Chief should assess resource needs assessment using the needs indicated by the Operations Section Chief and resources data available from the Planning Section's Resources Unit. The planning matrix, when properly completed, will show resource requirements and the resources available to meet those requirements. Subtracting the resources available from those required will indicate any additional resource needs. From this assessment, a new resource order can be developed and provided to the IC for approval and then placed through normal dispatch channels by the Logistics Section.

CONSIDER COMMUNICATIONS, MEDICAL, AND TRAFFIC PLAN REQUIREMENTS

The IAP will normally consist of the Incident Objectives (ICS 202), Organization Chart (ICS 203), Division Assignment List (ICS 204), and a map of the incident area. Larger incidents may require additional supporting attachments, such as a separate Communications Plan (ICS 205), a Medical Plan (ICS 206), and possibly a Traffic Plan. (For examples of ICS forms, see Appendix B, Tab 9.) The Planning Section Chief must determine the need for these attachments and ensure that the appropriate units prepare such attachments. For major incidents, the IAP and attachments will normally include the items listed in Table B-2.

Table B-2—The IAP and Typical Attachments

COMPONENTS	NORMALLY PREPARED BY
Common Components	
Incident Objectives (Form: ICS 202)	Incident Commander
Organization List or Chart (Form: ICS 203)	Resources Unit
Assignment List (Form: ICS 204)	Resources Unit
Communications Plan (Form: ICS 205)	Communications Unit
Responder Medical Plan (Form: ICS 206)	Medical Unit
Incident Map	Situation Unit
General Safety Message	Safety Officer
Other Potential Components (Incident dependent)	
Air Operations Summary	Air Operations
Traffic Plan	Ground Support Unit
Decontamination Plan	Technical Specialist
Waste Management or Disposal Plan	Technical Specialist
Demobilization Plan	Demobilization Unit
Evacuation Plan	Technical Specialist
Site Security Plan	Law Enforcement Technical Specialist or a Security Manager
Investigative Plan	Law Enforcement Technical Specialist
Evidence Recovery Plan	Law Enforcement Technical Specialist
Other	As Required

Prior to the completion of the plan, the Planning Section Chief should review the division and group tactical work assignments for any changes due to lack of resource availability.

The Resource Unit may then transfer division assignment information including alternatives from the planning matrix board or form onto the Division Assignment Lists (ICS 204).

FINALIZE, APPROVE, AND IMPLEMENT THE INCIDENT ACTION PLAN

The Planning Section is responsible for seeing that the IAP is completed, reviewed, and distributed. The following is the sequence of steps for accomplishing this:

- Set the deadline for completing IAP attachments.
- Obtain plan attachments and review them for completeness and approvals.
- Determine the number of IAPs required.
- Arrange with the Documentation Unit to reproduce the IAP.
- Review the IAP to ensure it is up to date and complete prior to the operations briefing and plan distribution.
- Provide the IAP briefing plan, as required, and distribute the plan prior to beginning of the new operational period.

Table B-3—ICS Forms that
Can Aid the Planning Process*

NUMBER	PURPOSE
ICS-201 (p.1)	Incident Briefing
ICS-201 (p.2)	Summary of Current Actions
ICS-201 (p.3)	Current Organization
ICS-201 (p.4)	Resources Summary
ICS-202	Incident Objectives
ICS-203	Organization Assignment List
ICS-204	Assignment List
ICS-205	Incident Radio Communications Plan
ICS-206	Medical Plan
ICS-207	Organizational Chart
ICS-209**	Incident Status Summary, with Instructions
ICS-210	Status Change Card
ICS-211	Check-In-List
ICS-213	General Message
ICS 215	Operational Planning Worksheet
ICS 215a	Incident Action Plan Safety Analysis

*ICS forms are guidance documents to assist in writing an agency's IAP. Some modification to the forms can be performed to better suit an agency's need so long as the nature of each form or numbering is not altered.

**ICS-209 is used by the NWCG.

TAB 9—EXAMPLES OF ICS FORMS

The following pages contain examples of the ICS Forms that are discussed in this document. These examples have been drawn from the U.S. Department of Agriculture's Forest Service; other emergency management organizations also provide ICS hardcopy forms and software packages to generate ICS forms that may be used for incident management purposes.

Table B-4—Examples of ICS Forms Included in this Tab

NUMBER	PURPOSE
ICS 201 (p.1)	Incident Briefing
ICS 201 (p.2)	Summary of Current Actions
ICS 201 (p.3)	Current Organization
ICS 201 (p.4)	Resource Summary
ICS 202	Incident Objectives
ICS 203	Organization Assignment List
ICS 204	Assignment List
ICS 205	Incident Radio Communications Plan
ICS 206	Medical Plan
ICS 211	Check-In List
ICS 215	Operational Planning Worksheet
ICS 215a	Incident Action Plan Safety Analysis

ICS FORMS

The following is a list of ICS forms. These forms are available online, commercially and in a variety of formats; however, all the examples listed are based on the original forms.[45]

[45] The ICS forms are under going an updating process and the new forms will be available online on the NIC website, after completion.

ICS 201 – Incident Briefing Form

The ICS 201–Incident Briefing Form is most often used by the initial Incident Commander and is a four-sheet document that allows for the capture of vital incident command and control information prior to the implementation of the formal planning process. This form allows for a concise and complete transition of Command briefing to an incoming new Incident Commander. In addition, this form may serve as the full extent of incident command and control documentation if the situation is resolved by the initial response resources and organization. This form is designed to be transferred easily to the members of the Command and General Staff as they arrive and begin work. It is not included as a part of the formal written Incident Action Plan.

ICS 202 – Incident Objectives

The ICS 202 – Incident Objectives serves as the first page of a written IAP. It includes incident information, a listing of the Incident Commander's Objectives for the Operational Period, pertinent weather information, a general safety message, and a table of contents for the plan. Signature Blocks are provided.

ICS 203 – Organizational Assignment List

The ICS 203 – Organizational Assignment List is typically the second page of the IAP and provides a full accounting of incident management and supervisory staff for that Operational Period.

ICS 204 – Division/Group Assignment List

The ICS 204 – Division/Group Assignment List is included in multiples based on the organizational structure of the Operations Section for the Operational Period. Each Division or Group will have its own page. This page will list who is supervising the Division or Group to include Branch Director if assigned. It will also list the specific assigned resources with leader name and number of personnel assigned to each resource. This document then describes in detail the specific actions that that Division or Group will be taking in support of the overall incident objectives. Any special instruction will be included as well as the elements of the communication plan that applies to that Division or Group.

ICS 205 – Incident Communications Plan

The ICS 205 – Incident Communications Plan depicts the entire communications plan for the incident.

ICS 206 – Incident Medical Plan

The ICS 206 – Incident Medical Plan presents the incident's medical plan to care for responder medical emergencies.

ICS 211 – Check-In List

The ICS 211 – Check-In List is used to document the check-in process. Check-in recorders report check-in information to the Resources Unit.

ICS 215 – Operational Planning Worksheet

The ICS 215 – Operational Planning Worksheet communicates to the Resources Unit the resources needed as a result of decisions made during the Tactics and Planning meetings. The Worksheet is used by the Resources Unit to complete the Assignment List (ICS 204) and by the Logistics Section Chief for ordering resources.

ICS 215a – Incident Action Plan Safety Analysis

The ICS 215a – Incident Action Plan Safety Analysis communicates to the Operations and Planning Section Chiefs safety and health issues identified by the Safety Officer. The Worksheet is used by the Resources Unit to complete ICS 204 Forms and Operations briefings.

INCIDENT BRIEFING	1. INCIDENT NAME	2. DATE PREPARED	3. TIME PREPARED
4. MAP SKETCH			
ICS 201 (12/93) NFES 1325	PAGE 1	5. PREPARED BY (NAME AND POSITION)	

Figure B-17—ICS 201 p.1

6. SUMMARY OF CURRENT ACTIONS		
ICS 201 (12/93) **NFES 1325**	PAGE 2	

Figure B-18—ICS 201 p.2

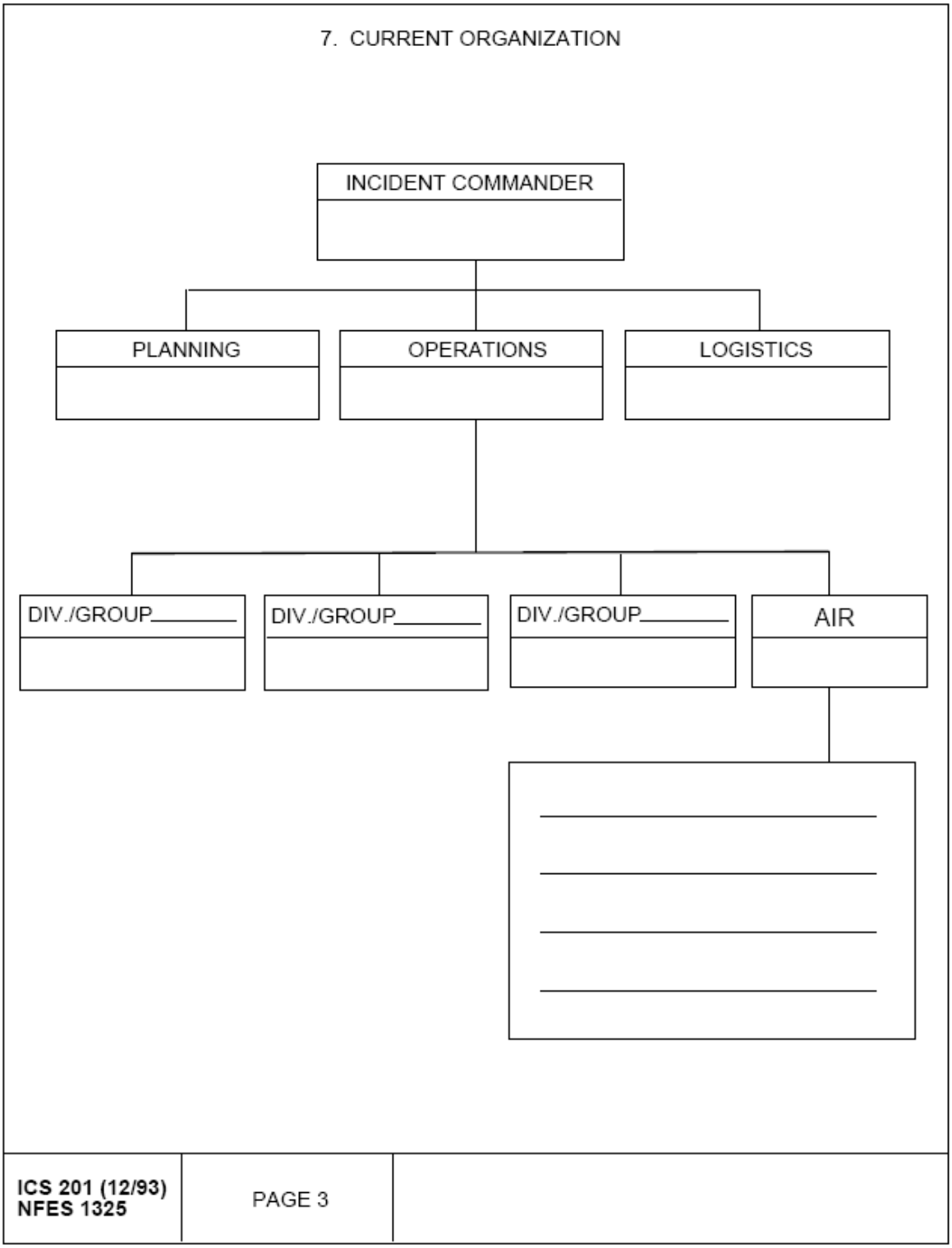


Figure B-19—ICS 201 p.3

8. RESOURCES SUMMARY				
RESOURCES ORDERED	RESOURCES IDENTIFICATION	ETA	ON SCENE √	LOCATION/ASSIGNMENT
ICS 201 (12/93) NFES 1325	PAGE 4			

1

Figure B-20—ICS 201 p.4

INCIDENT OBJECTIVES	1. INCIDENT NAME	2. DATE PREPARED	3. TIME PREPARED
4. OPERATIONAL PERIOD (DATE/TIME)			
5. GENERAL CONTROL OBJECTIVES FOR THE INCIDENT (INCLUDE ALTERNATIVES)			
6. WEATHER FORECAST FOR OPERATIONAL PERIOD			
7. GENERAL SAFETY MESSAGE			
8. ATTACHMENTS (✓ IF ATTACHED) ☐ ORGANIZATION LIST (ICS 203) ☐ MEDICAL PLAN (ICS 206) ☐ _____ ☐ ASSIGNMENT LIST (ICS 204) ☐ INCIDENT MAP ☐ _____ ☐ COMMUNICATIONS PLAN (ICS 205) ☐ TRAFFIC PLAN ☐ _____			
9. PREPARED BY (PLANNING SECTION CHIEF)	10. APPROVED BY (INCIDENT COMMANDER)		

Figure B-21—ICS 202

ORGANIZATION ASSIGNMENT LIST	1. INCIDENT NAME	2. DATE PREPARED	3. TIME PREPARED
POSITION / NAME	4. OPERATIONAL PERIOD (DATE/TIME)		

5. INCIDENT COMMANDER AND STAFF

INCIDENT COMMANDER	
DEPUTY	
SAFTEY OFFICER	
INFORMATION OFFICER	
LIAISON OFFICER	

6. AGENCY REPRESENTATIVES

AGENCY	NAME

7. PLANNING SECTION

CHIEF	
DEPUTY	
RESOURCES UNIT	
SITUATION UNIT	
DOCUMENTATION UNIT	
DEMOBILIZATION UNIT	
TECHNICAL SPECIALISTS	

8. LOGISTICS SECTION

CHIEF	
DEPUTY	
a. SUPPORT BRANCH	
DIRECTOR	
SUPPLY UNIT	
FACILITIES UNIT	
GROUND SUPPORT UNIT	
b. SERVICE BRANCH	
DIRECTOR	
COMMUNICATIONS UNIT	
MEDICAL UNIT	
FOOD UNIT	

9. OPERATIONS SECTION

CHIEF	
DEPUTY	
a. BRANCH I- DIVISION/GROUPS	
BRANCH DIRECTOR	
DEPUTY	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
b. BRANCH II- DIVISION/GROUPS	
BRANCH DIRECTOR	
DEPUTY	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
c. BRANCH III- DIVISION/GROUPS	
BRANCH DIRECTOR	
DEPUTY	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
DIVISION/GROUP	
d. AIR OPERATIONS BRANCH	
AIR OPERATIONS BR. DIR.	
AIR TACTICAL GROUP SUP.	
AIR SUPPORT GROUP SUP.	
HELICOPTER COORDINATOR	
AIR TANKER/FIXED WING CRD.	

10. FINANCE/ADMINISTRATION SECTION

CHIEF	
DEPUTY	
TIME UNIT	
PROCUREMENT UNIT	
COMPENSATION/CLAIMS UNIT	
COST UNIT	

PREPARED BY(RESOURCES UNIT)

Figure B-22—ICS 203

1. BRANCH	2. DIVISION/GROUP	**ASSIGNMENT LIST**
3. INCIDENT NAME	4. OPERATIONAL PERIOD DATE _____ TIME _____	

5. OPERATIONAL PERSONNEL

OPERATIONS CHIEF _____ DIVISION/GROUP SUPERVISOR _____

BRANCH DIRECTOR _____ AIR TACTICAL GROUP SUPERVISOR _____

6. RESOURCES ASSIGNED THIS PERIOD

STRIKE TEAM/TASK FORCE/ RESOURCE DESIGNATOR	EMT	LEADER	NUMBER PERSONS	TRANS. NEEDED	PICKUP PT./TIME	DROP OFF PT./TIME

7. CONTROL OPERATIONS

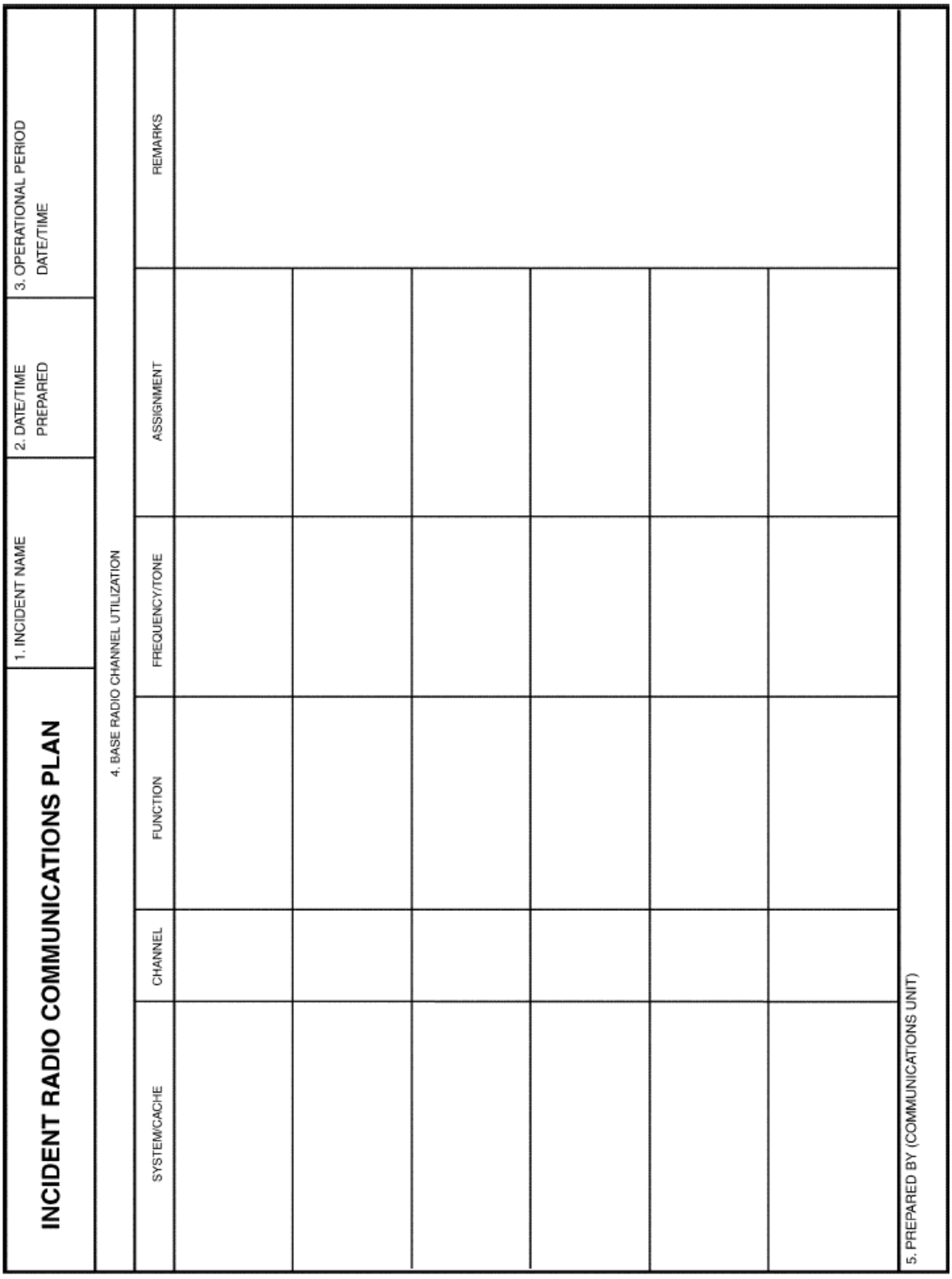
8. SPECIAL INSTRUCTIONS

9. DIVISION/GROUP COMMUNICATIONS SUMMARY

FUNCTION		FREQ.	SYSTEM	CHAN.	FUNCTION		FREQ.	SYSTEM	CHAN.
COMMAND	LOCAL				SUPPORT	LOCAL			
	REPEAT					REPEAT			
DIV./GROUP TACTICAL					GROUND TO AIR				

PREPARED BY (RESOURCE UNIT LEADER)	APPROVED BY (PLANNING SECT. CH.)	DATE	TIME

Figure B-23—ICS 204



INCIDENT RADIO COMMUNICATIONS PLAN

1. INCIDENT NAME	2. DATE/TIME PREPARED	3. OPERATIONAL PERIOD DATE/TIME

4. BASE RADIO CHANNEL UTILIZATION

SYSTEM/CACHE	CHANNEL	FUNCTION	FREQUENCY/TONE	ASSIGNMENT	REMARKS

5. PREPARED BY (COMMUNICATIONS UNIT)

Figure B-24—ICS 205

MEDICAL PLAN	1. Incident Name	2. Date Prepared	3. Time Prepared	4. Operational Period

5. Incident Medical Aid Station

Medical Aid Stations	Location	Paramedics Yes	Paramedics No

6. Transportation

A. Ambulance Services

Name	Address	Phone	Paramedics Yes	Paramedics No

B. Incident Ambulances

Name	Location	Paramedics Yes	Paramedics No

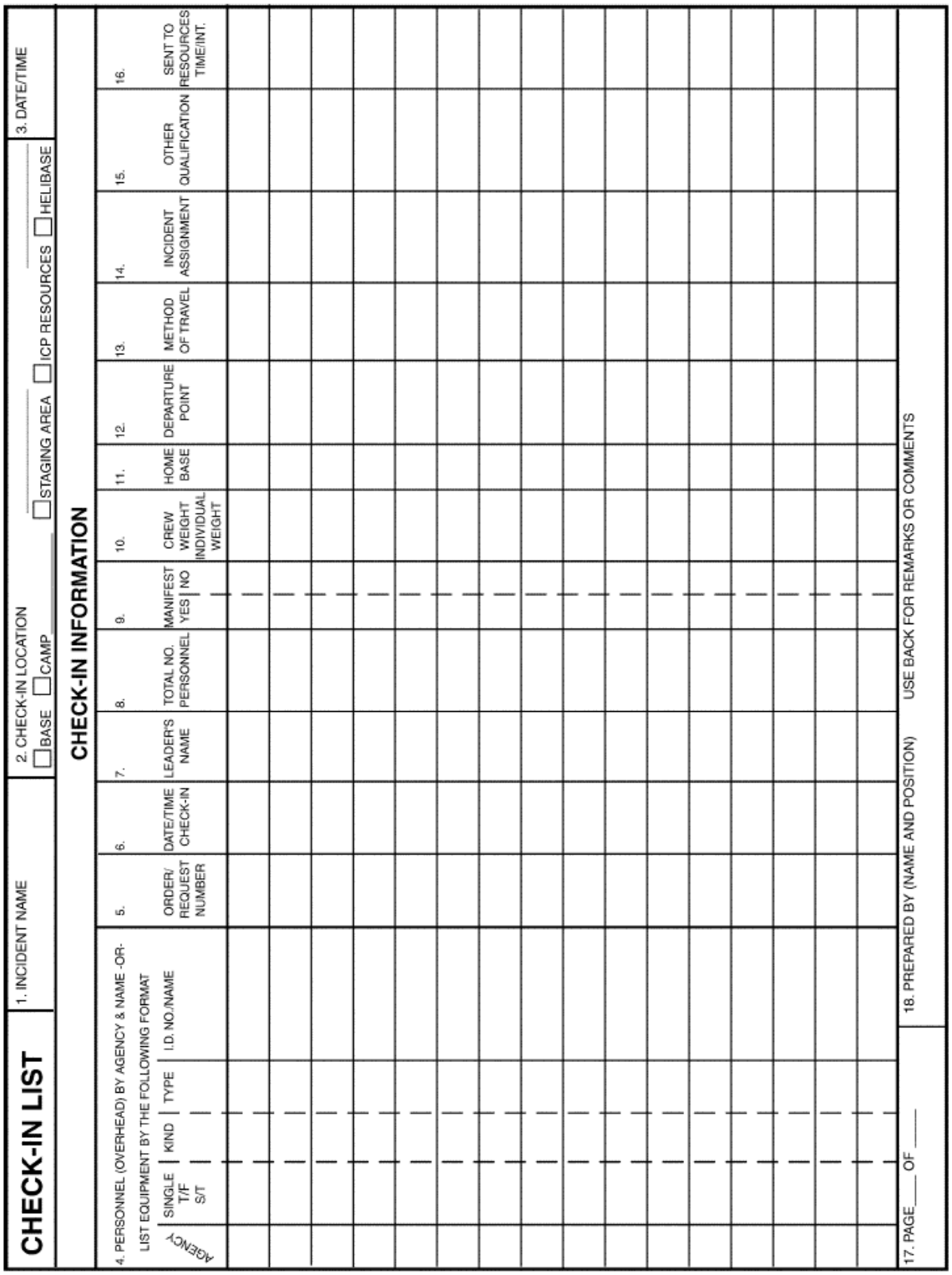
7. Hospitals

Name	Address	Travel Time Air	Travel Time Ground	Phone	Helipad Yes	Helipad No	Burn Center Yes	Burn Center No

8. Medical Emergency Procedures

Prepared by (Medical Unit Leader)	10. Reviewed by (Safety Officer)

Figure B-25—ICS 206



CHECK-IN LIST

1. INCIDENT NAME

2. CHECK-IN LOCATION ☐BASE ☐CAMP_____ ☐STAGING AREA_____ ☐ICP RESOURCES ☐HELIBASE_____

3. DATE/TIME

CHECK-IN INFORMATION

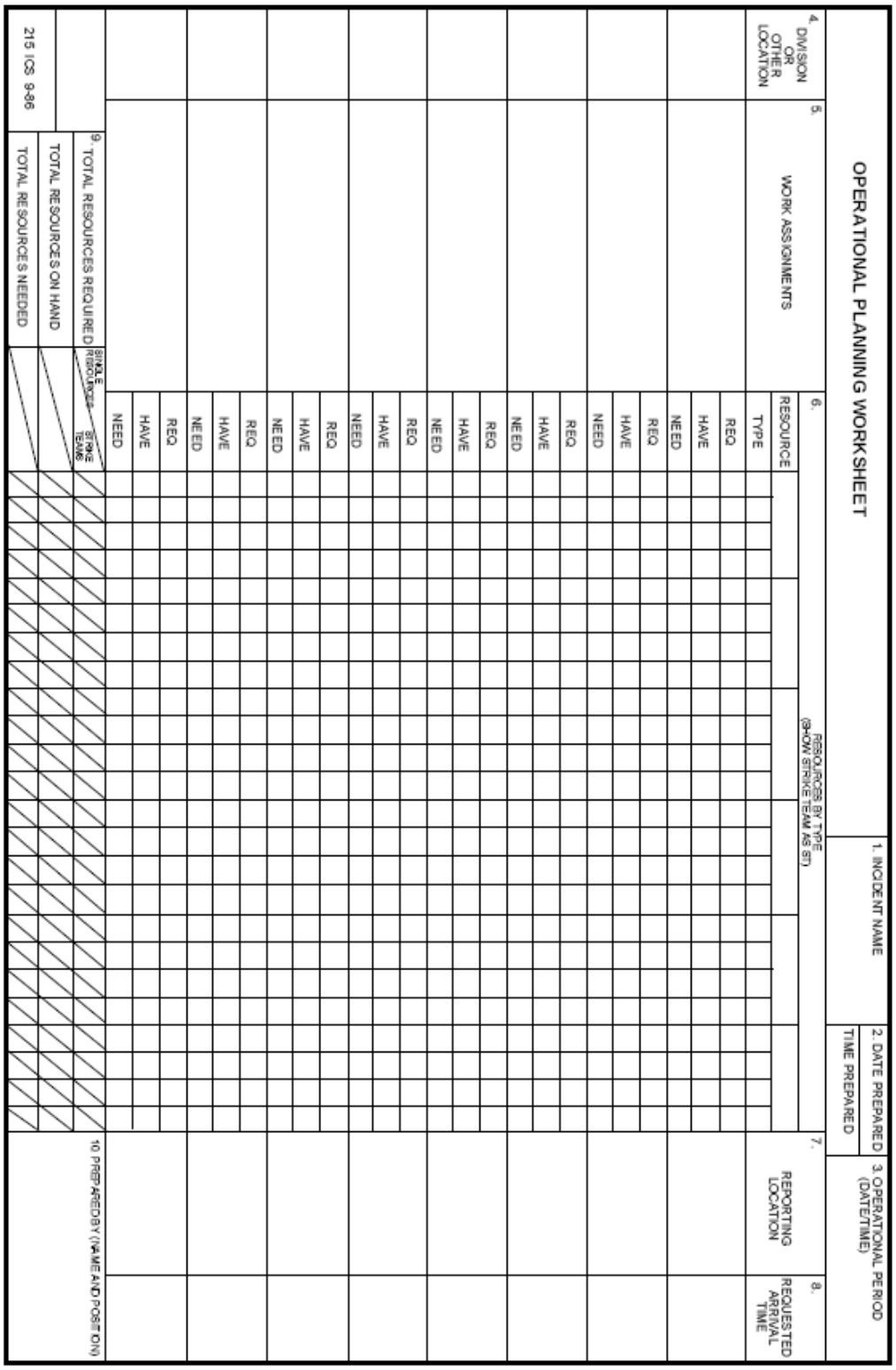
4. PERSONNEL (OVERHEAD) BY AGENCY & NAME -OR- LIST EQUIPMENT BY THE FOLLOWING FORMAT				5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
AGENCY	SINGLE T/F S/T	KIND	TYPE	I.D. NO./NAME	ORDER/ REQUEST NUMBER	DATE/TIME CHECK-IN	LEADER'S NAME	TOTAL NO. PERSONNEL	MANIFEST YES NO	CREW WEIGHT INDIVIDUAL WEIGHT	HOME BASE	DEPARTURE POINT	METHOD OF TRAVEL	INCIDENT ASSIGNMENT	OTHER QUALIFICATION	SENT TO RESOURCES TIME/INT.

17. PAGE___ OF ____

18. PREPARED BY (NAME AND POSITION)

USE BACK FOR REMARKS OR COMMENTS

Figure B-26—ICS 211



OPERATIONAL PLANNING WORKSHEET

1. INCIDENT NAME | 2. DATE PREPARED / TIME PREPARED | 3. OPERATIONAL PERIOD (DATE/TIME)

4. DIVISION OR OTHER LOCATION

5. WORK ASSIGNMENTS

6. RESOURCES BY TYPE (SHOW STRIKE TEAM AS ST)

RESOURCE TYPE: REQ / HAVE / NEED

7. REPORTING LOCATION

8. REQUESTED ARRIVAL TIME

9. TOTAL RESOURCES REQUIRED (SINGLE RESOURCES / STRIKE TEAMS): REQ / HAVE / NEED

TOTAL RESOURCES ON HAND

TOTAL RESOURCES NEEDED

10. PREPARED BY (NAME AND POSITION)

215 ICS 9-86

1

1 Figure B-27—ICS 215

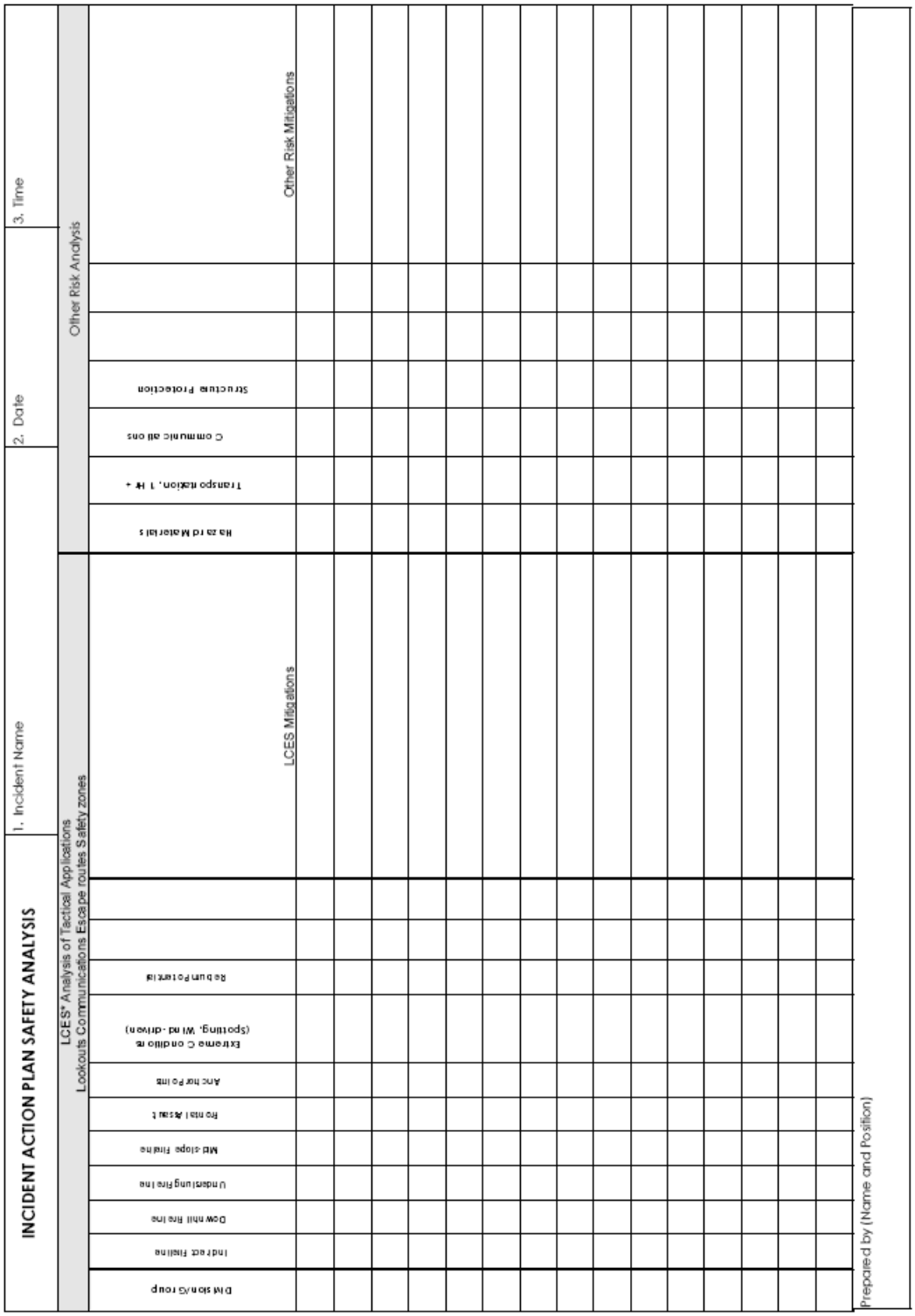


Figure B-28—ICS 215a

APPENDIX C

SUMMARY OF MAJOR ICS POSITIONS

SUMMARY TABLE OF MAJOR ICS POSITIONS

[Adapted from ICS-400 course, Module 12]

MAJOR ICS POSITIONS	PRIMARY FUNCTIONS
Incident Command: Incident Commander (IC) or Unified Command (UC)	• Have clear authority and know agency policy • Ensure incident safety • Establish ICP • Set priorities, determine incident objectives and strategies to be followed • Establish ICS organization needed to manage the incident • Approve IAP • Coordinate Command & General staff activities • Approve resource requests and use of volunteers and auxiliary personnel • Order demobilization as needed • Ensure after-action reports are completed
Public Information Officer (PIO)	• Determine, according to direction from the IC, any limits on information release • Develop information for use in press/media briefings • Obtain IC's approval of media news releases • Conduct periodic media briefings • Arrange for tours and other interviews or briefings that may be required • Monitor and forward media information that may be useful to incident planning • Maintain current information summaries and/or displays on the incident • Make information about the incident available to incident personnel • Participate in the planning meeting
Safety Officer (SO)	• Identify and mitigate hazardous situations • Ensure safety messages and briefings are made

	• Exercise emergency authority to stop and prevent unsafe acts Review the IAP for safety implications • Assign assistants qualified to evaluate special hazards • Initiate preliminary investigation of accidents within the incident area • Review and approve the Medical Plan • Participate in planning meetings
Liaison Officer (LNO)	• Act as a point of contact for Agency Reps • Maintain a list of assisting and cooperating agencies and Agency Reps • Assist in setting up and coordinating inter-agency contacts • Monitor incident operations to identify current or potential inter-organizational problems • Participate in planning meetings, providing current resource status, including limitations and capability of agency resources • Provide agency-specific demobilization information and requirements
Operations Section Chief (OSC)	• Manage tactical operations • Assure safety of tactical operations • Assist with the operations portions of the IAP • Supervise execution of operations portions of IAP • Request additional resources to support tactical operations • Approve release of resources of active operational assignments • Make or approve expedient changes to the IAP • Maintain close contact with IC, subordinate Ops personnel, and other agencies involved in the incident.
Plans Section Chief (PSC)	• Collect and manage all incident-relevant operational data • Supervise preparation of the IAP • Provide input to the IC and Ops in preparing IAP • Incorporate traffic, medical, communications plans and other supporting material into the IAP Conduct and facilitate planning meetings • Reassign personnel within ICS organization • Compile and display incident status information Establish information requirements and reporting schedules for units (e.g., resources, situation units) • Determine need for specialized resources • Assemble and disassemble task forces and strike teams not assigned to Ops • Establish specialized data collection systems as necessary (e.g.,

	weather) • Assemble information on alternative strategies • Provide periodic predictions on incident potential • Report significant changes in incident status • Oversee preparation of the Demobilization Plan
Logistics Section Chief (LSC)	• Provide all facilities, transportation, communications, supplies, equipment maintenance and fueling, food and medical services for incident personnel, and all off-incident resources • Manage all incident logistics • Provide logistics input to the IAP • Brief Logistics staff as needed • Identify anticipated and known incident service and support requirements • Request additional resources as needed • Develop as required the Communications, Medical, and Traffic plans • Oversee demobilization of Logistics section and associated resources
Finance/Admin Section Chief (FSC)	• Manage all financial aspects of an incident • Provide financial and cost analysis information as requested • Ensure compensation and claims functions are being addressed relative to the incident • Gather pertinent information from briefings with responsible agencies • Develop an operation plan for the Finance/Administration Section and fill Section supply and support needs • Determine need to set up and operate an incident commissary • Meet with assisting and cooperating agency reps as needed • Maintain daily contact with agency(s) HQ on finance matters • Ensure that personnel time records are accurately complete and transmitted to home agencies • Ensure that all obligation documents initiated at the incident are properly prepared and completed • Brief agency administrative personnel on all incident-related financial issues needing attention or follow-up

*Information and Intelligence functions may be under the direction of a separate General Staff position, Information and Intelligence Section Chief (INTEL). Usually these functions are part of Operations and/or Planning sections.

GLOSSARY OF KEY TERMS

For the purposes of the NIMS, the following terms and definitions apply:

Air Operations Branch: The Operations Section Chief may establish an Air Operations Branch to meet mission requirements in certain situations, in which size, organization, and operation will depend primarily on the nature of the incident and the availability of air assets.

Acquisition Procedures: Used to obtain resources to support operational requirements.

Accreditation: Empowers certifying/qualifying organizations with the authority to declare an individual capable of performing critical tasks and capabilities.

Agency: A division of government with a specific function offering a particular kind of assistance. In ICS, agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance).

Agency Administrator or Executive: The official responsible for administering policy for an agency or jurisdiction, having full authority for making decisions and providing direction to the management organization for an incident.

Agency Dispatch: The agency or jurisdictional facility from which resources are allocated to incidents.

Agency Representative: A person assigned by a primary, assisting, or cooperating Federal, State, local, or Tribal government agency or private entity that has been delegated authority to make decisions affecting that agency's or entity's participation in incident management activities following appropriate consultation with the leadership of that agency.

Air Operations Branch Director: The person primarily responsible for preparing and implementing the air operations portion of the Incident Action Plan. Also responsible for providing logistical support to helicopters operating on the incident.

Allocated Resources: Resources dispatched to an incident.

All-hazards: Any incident or event, natural or human-caused that warrants action to protect life, property, environment, public health or safety, and minimize disruptions of government, social or economic activities.

Area Command (Unified Area Command): An organization established (1) to oversee the management of multiple incidents that are each being handled by an ICS organization or (2) to oversee the management of large or multiple incidents to which several Incident Management Teams have been assigned. Area Command has the responsibility to set overall strategy and priorities, allocate critical

resources according to priorities, ensure that incidents are properly managed, and ensure that objectives are met and strategies followed. Area Command becomes Unified Area Command when incidents are multi-jurisdictional. Area Command may be established at an emergency operations center facility or at some location other than an incident command post.

Assessment: The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Assigned Resources: Resources checked in and assigned work tasks on an incident.

Assignments: Tasks given to resources to perform within a given operational period that are based on operational objectives defined in the IAP.

Assistant: Title for subordinates of principal Command Staff positions. The title indicates a level of technical capability, qualifications, and responsibility subordinate to the primary positions. Assistants may also be assigned to unit leaders.

Assisting Agency: An agency or entity providing personnel, services, or other resources to the agency with direct responsibility for incident management. See also Supporting Agency.

Available Resources: Resources assigned to an incident, checked in, and available for a mission assignment, normally located in a Staging Area.

Badging: Based on credentialing and resource ordering, provides incident-specific credentials and can be used to limit access to various incident sites.

Backup Management Information Systems: Management information systems should have redundancy of power supply and communication lines. But resource managers should also identify alternate backup systems to manage resources, in the event that the primary resource management system is disrupted by incident conditions.

Base: The location at which primary Logistics functions for an incident are coordinated and administered. There is only one Base per incident. (Incident name or other designator will be added to the term Base.) The Incident Command Post may be co-located with the Base.

Branch: The organizational level having functional or geographical responsibility for major aspects of incident operations. A branch is organizationally situated between the section and the division or group in the Operations Section, and between the section and units in the Logistics Section. Branches are identified by the use of Roman numerals or by functional area.

Cache: A pre-determined complement of tools, equipment, and/or supplies stored in a designated location, available for incident use.

Camp: A geographical site, within the general incident area, separate from the Incident Base, equipped and staffed to provide sleeping, food, water, and sanitary services to incident personnel.

Catastrophic incidents: Any natural or manmade incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic incident could result in sustained national impacts over a prolonged period of time; almost immediately

exceeds resources available to State, local, Tribal, and private sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened. All catastrophic events are Incidents of National Significance.

Categorizing Resources: Resources are categorized by size, capacity, capability, skill, and other characteristics. This makes the resource ordering and dispatch process within jurisdictions, across jurisdictions, and between governmental and non-governmental entities more efficient and ensures that Incident Command receives resources appropriate to their needs.

Certifying Personnel: Personnel certification entails authoritatively attesting that individuals meet professional standards for the training, experience, and performance required for key incident management functions.

Chain of Command: A series of command, control, executive, or management positions in hierarchical order of authority.

Check-In: The process through which resources first report to an incident. Check-in locations include the incident command post, Resources Unit, incident base, camps, staging areas, or directly on the site.

Chief: The ICS title for individuals responsible for management of functional sections: Operations, Planning, Logistics, Finance/Administration, and Intelligence (if established as a separate section).

Command: The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority.

Command Staff: In an incident management organization, the Command Staff consists of the Incident Command and the special staff positions of Public Information Officer, Safety Officer, Liaison Officer, and other positions as required, who report directly to the Incident Commander. They may have an assistant or assistants, as needed.

Common Operating Picture: A broad view of the overall situation as reflected by situation reports, aerial photography, and other information or intelligence.

Communications Unit: An organizational unit in the Logistics Section responsible for providing communication services at an incident or an EOC. A Communications Unit may also be a facility (e.g., a trailer or mobile van) used to support an Incident Communications Center.

Compacts: Formal working agreements among agencies to obtain mutual aid.

Complex: Two or more individual incidents located in the same general area that are assigned to a single Incident Commander or to Unified Command.

Cooperating Agency: An agency supplying assistance other than direct operational or support functions or resources to the incident management effort.

Coordinate: To advance systematically an analysis and exchange of information among principals who have or may have a need to know certain information to carry out specific incident management responsibilities.

Corrective Action and Mitigation Plans: Corrective action plans are designed to implement procedures that are based on lessons learned from actual incidents or from training and exercises.

Mitigation plans describe activities that can be taken prior to, during, or after an incident to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.

Cost Unit: Functional Unit within the Finance/Administration Section responsible for tracking costs, analyzing cost data, making cost estimates, and recommending cost-saving measures.

Credentialing: Involves providing documentation that can authenticate and verify the certification and identity of designated incident managers and emergency responders.

Delegation of Authority: A statement provided to the Incident Commander by the Agency Executive delegating authority and assigning responsibility. The Delegation of Authority can include objectives, priorities, expectations, constraints, and other considerations or guidelines as needed. Many agencies require written Delegation of Authority to be given to Incident Commanders prior to their assuming command on larger incidents.

Demobilization Unit: Functional Unit within the Planning Section responsible for assuring orderly, safe, and efficient demobilization of incident resources.

Deputy: A fully qualified individual who, in the absence of a superior, can be delegated the authority to manage a functional operation or perform a specific task. In some cases, a deputy can act as relief for a superior and, therefore, must be fully qualified in the position. Deputies can be assigned to the Incident Commander, General Staff, and Branch Directors.

Director: The ICS title for individuals responsible for supervision of a Branch.

Disaster Recovery Center (DRC): A satellite component of the JFO and provides a central facility where individuals affected by a disaster can obtain information on disaster recovery assistance programs from various Federal, State, local, Tribal, private sector, and voluntary organizations.

Dispatch: The ordered movement of a resource or resources to an assigned operational mission or an administrative move from one location to another.

Division: The partition of an incident into geographical areas of operation. Divisions are established when the number of resources exceeds the manageable span of control of the Operations Chief. A division is located within the ICS organization between the Branch and resources in the Operations Section.

Documentation Unit: Functional Unit within the Planning Section responsible for collecting, recording, and safeguarding all documents relevant to the incident.

Emergency: Absent a Presidential-declared emergency, any incident(s), human-caused or natural, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.

Emergency Operations Centers (EOCs): The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally

takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, Tribal), or some combination thereof.

Emergency Management Assistance Compact (EMAC): Is a congressionally ratified organization that provides form and structure to interstate mutual aid. Through EMAC, a disaster impacted state can request and receive assistance from other member states quickly and efficiently, resolving two key issues upfront: liability and reimbursement.

Emergency Operations Plan: The "steady-state" plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

Emergency Public Information: Information that is disseminated primarily in anticipation of an emergency or during an emergency. In addition to providing situational information to the public, it also frequently provides directive actions required to be taken by the general public.

Emergency Response Provider: Includes Federal, State, local, and Tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities. See Section 2 (6), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002). Also known as Emergency Responder.

Evacuation: Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

Event: A planned, non-emergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.

Facilities Unit: Functional Unit within the Support Branch of the Logistics Section that provides fixed facilities for the incident. These facilities may include the Incident Base, feeding areas, sleeping areas, sanitary facilities, etc.

Federal: Of or pertaining to the Federal Government of the United States of America.

Field Operations Guide (FOG) or Handbook: A durable pocket or desk guide that contains essential information required to perform specific assignments or functions.

Finance/Administration Section: The section responsible for all administrative and financial considerations surrounding an incident.

Food Unit: Functional Unit within the Service Branch of the Logistics Section responsible for providing meals for incident personnel.

Function: Function refers to the five major activities in ICS: Command, Operations, Planning, Logistics, and Finance/Administration. The term function is also used when describing the activity involved, e.g., the planning function. A sixth function, Intelligence, may be established, if required, to meet incident management needs.

General Staff: A group of incident management personnel organized according to function and reporting to the Incident Commander. The General Staff normally consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief.

Ground Support Unit: Functional Unit within the Support Branch of the Logistics Section responsible for the fueling, maintaining, and repairing of vehicles, and the transportation of personnel and supplies.

Group: Established to divide the incident management structure into functional areas of operation. Groups are composed of resources assembled to perform a special function not necessarily within a single geographic division. Groups, when activated, are located between Branches and resources in the Operations Section. (see Division.)

Hazard: Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Identification and Authentication: Individuals and organizations that access the NIMS information management system and, in particular, those that contribute information to the system (e.g., situation reports), must be properly authenticated and certified for security purposes.

Incident: An occurrence or event, natural or human-caused that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Incident Action Plan (IAP): An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods.

Incident Commander (IC): The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

Incident Command Post (ICP): The field location at which the primary tactical-level, on-scene incident command functions are performed. The ICP may be co-located with the incident base or other incident facilities and is normally identified by a green rotating or flashing light.

Incident Command System (ICS): A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small as well as large and complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations.

Incident Communications: Incident Command manages communications at an incident, using a common communications plan and an incident-based communications center established solely for use by the command, tactical, and support resources assigned to the incident. All entities involved in managing the incident will utilize common terminology, prescribed by the NIMS, for communications.

Incident Management: The broad spectrum of activities and organizations providing effective and efficient operations, coordination and support applied at all levels of government, utilizing both governmental and non-governmental resources, to plan for, respond to and recover from an incident regardless of cause, size, or complexity.

Incident Management Team (IMT): An IC and appropriate Command and General Staff personnel assigned to an incident. IMTs are generally grouped in five types. Types I and II are National teams, Type III are State or regional, Type IV are discipline or large jurisdiction specific, while Type V are ad hoc incident command organizations, typically used by smaller jurisdictions.

Incident Objectives: Statements of guidance and direction necessary for selecting appropriate strategy(s) and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow strategic and tactical alternatives.

Incident of National Significance (INS): An actual or potential high-impact incident that requires robust coordination of the Federal response in order to save lives and minimize damage, and provide the basis for long-term community and economic recovery.

- The Secretary of Homeland Security, in consultation with other departments and agencies, and the White House, as appropriate, declares Incidents of National Significance.
- There are no automatic triggers for an Incident of National Significance.
- The Secretary of Homeland Security will manage the Federal government's response following the declaration of an Incident of National Significance.

Incident Support Organization: Includes any off-incident support provided to an incident. Examples would be Agency Dispatch centers, Airports, Mobilization Centers, etc.

Initial Action: The actions taken by those responders first to arrive at an incident site.

Initial Response: Resources initially committed to an incident.

Intelligence Officer: The intelligence officer is responsible for managing internal information, intelligence, and operational security requirements supporting incident management activities. These may include information security and operational security activities, as well as the complex task of ensuring that sensitive information of all types (e.g., classified information, law enforcement sensitive information, proprietary information, or export-controlled information) is handled in a way that not only safeguards the information, but also ensures that it gets to those who need access to it to perform their missions effectively and safely.

Job Aid: A checklist or other aid that is useful in performing or training for a job.

Joint Field Office (JFO): A temporary Federal facility established locally to provide a central point for Federal, State, local, and Tribal executives with responsibility for incident oversight, direction, and/or assistance to effectively coordinate protection, prevention, preparedness, response, and recovery actions.

Joint Field Office Coordination Group: The JFO Coordination Group functions as a multi-agency coordination entity and works jointly to establish priorities (single or multiple incidents) and associated resource allocation, resolve agency policy issues, and provide strategic guidance to support Federal incident management activities. When activated, the JFO works in coordination with the State, county, and local EOCs to support incident management efforts.

Joint Information Center (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media at the scene of the incident. Public information officials from all participating agencies should co-locate at the JIC.

Joint Information System (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, timely information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated inter-agency messages; developing, recommending, and executing public information plans and strategies on behalf of the IC; advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.

Jurisdiction: A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, Tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health).

Jurisdictional Agency: The agency having jurisdiction and responsibility for a specific geographical area, or a mandated function.

Liaison: A form of communication for establishing and maintaining mutual understanding and cooperation.

Liaison Officer: A member of the Command Staff responsible for coordinating with representatives from cooperating and assisting agencies.

Local Government: A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or inter-state government entity, or agency or instrumentality of a local government; an Indian tribe or authorized Tribal entity, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. See Section 2 (10), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Logistics: Providing resources and other services to support incident management.

Logistics Section: The section responsible for providing facilities, services, and material support for the incident.

Major Disaster: As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, Tribes, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Managers: Individuals within ICS organizational Units that are assigned specific managerial responsibilities, e.g., Staging Area Manager or Camp Manager.

Management by Objective: A management approach that involves a four-step process for achieving the incident goal. The Management by Objectives approach includes the following: establishing overarching objectives; developing and issuing assignments, plans, procedures, and protocols; establishing specific, measurable objectives for various incident management functional activities and directing efforts to fulfill them, in support of defined strategic objectives; and documenting results to measure performance and facilitate corrective action.

Management Information Systems: Used to collect, update, and process data; track resources; and display their readiness status. Management information systems should incorporate resource accounting that anticipates reimbursement requirements.

Medical Unit: Functional Unit within the Service Branch of the Logistics Section responsible for the development of the Incident Medical Plan, and for providing emergency medical treatment of incident personnel and as required establish rest and rehabilitation for incident personnel.

Metrics: Measurable standards which are useful in describing a resource's capability.

Mitigation: The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

Mobilization: The process and procedures used by all organizations—Federal, State, local, and Tribal—for activating, assembling, and transporting all resources that have been requested to respond to or support an incident.

Multi-agency coordination entity: A multi-agency coordination entity functions within a broader multi-agency coordination system. It may establish the priorities among incidents and associated

resource allocations, deconflict agency policies, and provide strategic guidance and direction to support incident management activities.

Multi-Agency Coordination Systems: Multi-agency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The components of multi-agency coordination systems include facilities, equipment; emergency operation centers (EOCs), specific multi-agency coordination entities, personnel, procedures, and communications. These systems assist agencies and organizations to fully integrate the subsystems of the NIMS.

Multi-Jurisdictional Incident: An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under Unified Command.

Mutual-Aid Agreement: Written agreement between agencies and/or jurisdictions that they will assist one another on request, by furnishing personnel, equipment, and/or expertise in a specified manner.

National: Of a nationwide character, including the Federal, State, local, and Tribal aspects of governance and polity.

National Database of Incident Reports: Through the NIMS Integration Center, Federal, State, local, and Tribal organizations responsible for receiving initial incident reports will work collaboratively to develop and adopt a national database of incident reports that can be used to support incident management efforts.

National Disaster Medical System: A cooperative, asset-sharing partnership between the Department of Health and Human Services, the Department of Veterans Affairs, the Department of Homeland Security, and the Department of Defense. NDMS provides resources for meeting the continuity of care and mental health services requirements of the Emergency Support Function 8 in the Federal Response Plan.

National Incident Management System: A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and Tribal governments; the private sector, and NGOs to work effectively and efficiently together to prepare for, respond to, and recover from incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, local, and Tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

National Response Plan: A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.

Non-governmental Organization: An entity with an association that is based on interests of its members, individuals, or institutions and that is not created by a government, but may work

cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross.

Officer: The ICS title for the personnel responsible for the Command Staff positions of Safety, Liaison, and Public Information.

Operational Period: The time scheduled for executing a given set of operation actions, as specified in the Incident Action Plan. Operational periods can be of various lengths, although usually not over 24 hours.

Operations Section Chief: The Operations Section Chief directly manages all incident tactical activities and implements the Incident Action Plan.

Operations Section: The section responsible for all tactical incident operations. In ICS, it normally includes subordinate Branches, divisions, and/or groups.

Personnel Accountability: The ability to account for the location and welfare of incident personnel. It is accomplished when supervisors ensure that ICS principles and processes are functional and that personnel are working within established incident management guidelines.

Planning Meeting: A meeting held as needed prior to and throughout the duration of an incident to select specific strategies and tactics for incident control operations and for service and support planning. For larger incidents, the planning meeting is a major element in the development of the Incident Action Plan (IAP).

Planning Section: Responsible for the collection, evaluation, and dissemination of operational information related to the incident, and for the preparation and documentation of the IAP. This section also maintains information on the current and forecasted situation and on the status of resources assigned to the incident.

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.

Preparedness Organizations: The groups that provide inter-agency coordination for incident management activities in a non-emergency context. Preparedness organizations can include all agencies with a role in incident management, for prevention, preparedness, response, or recovery activities. They represent a wide variety of committees, planning groups, and other organizations that meet and coordinate to ensure the proper level of planning, training, equipping, and other preparedness requirements within a jurisdiction or area.

Preparedness Programs: Individual jurisdictions establish programs that address the requirements for each step of the preparedness cycle (planning, training, equipping, exercising, evaluating, and taking

action to correct and mitigate). These programs should adopt relevant NIMS standards, guidelines, processes, and protocols.

Prevention: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Private Sector: Organizations and entities that are not part of any governmental structure. It includes for-profit and not-for-profit organizations, formal and informal structures, commerce and industry, and private voluntary organizations (PVO).

Press Secretary: Someone typically associated with a political official, who will typically conjoin politician's interest with the apparent success of incident response.

Processes: Systems of operations that incorporate standardized procedures, methodologies, and functions necessary to provide resources effectively and efficiently. These include resource typing, resource ordering and tracking, and coordination.

Procurement Unit: Functional Unit within the Finance/Administration Section responsible for financial matters involving vendor contracts.

Public Information Officer: A member of the Command Staff responsible for interfacing with the public and media or with other agencies with incident-related information requirements.

Public Information Systems: These refer to processes, procedures, and systems for communicating timely and accurate information to the public during crisis or emergency situations.

Public Relations Officer: Similar to a press secretary, but representing an agency.

Publications Management: The publications management sub-system includes materials development, publication control, publication supply, and distribution. The development and distribution of NIMS materials is managed through this subsystem. Consistent documentation is critical to success, because it ensures that all responders are familiar with the documentation used in a particular incident regardless of the location or the responding agencies involved.

Qualification and Certification: This subsystem provides recommended qualification and certification standards for emergency responder and incident management personnel. It also allows the development of minimum standards for resources expected to have an inter-state application. Standards typically include training, currency, experience, and physical and medical fitness.

Recovery: The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic

restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

Recovery Plan: A plan developed by a State, local, or Tribal jurisdiction with assistance from responding Federal agencies to restore the affected area.

Regional Response Coordination Center (RRCC): A standing facility operated by DHS/FEMA that coordinates regional response efforts, establishes Federal priorities, and implements local Federal program support until a JFO is established in the field and/or other key DHS incident management officials can assume their NRP coordination responsibilities. The RRCC establishes communications with the affected State Emergency Operations Center (EOC) and the NOC-NRCC, coordinates deployment of the (Federal Advanced Teams/Individuals) to field locations, assesses damage information, develops situation reports, and issues initial mission assignments.

Reimbursement: Reimbursement provides a mechanism to fund critical needs that arise from incident-specific activities. Reimbursement processes also play an important role in establishing and maintaining the readiness of resources.

Resources: Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC.

Resource Identification and Ordering: Resource managers use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities.

Resource Management: Efficient incident management requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under the NIMS includes mutual-aid agreements; the use of special Federal, State, local, and Tribal teams; and resource mobilization protocols.

Resources Unit: Functional unit within the Planning Section responsible for recording the status of resources committed to the incident. This unit also evaluates resources currently committed to the incident, the effects additional responding resources will have on the incident, and anticipated resource needs.

Response: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting,

interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Safety Officer: A member of the Command Staff responsible for monitoring and assessing safety hazards or unsafe situations and for developing measures for ensuring personnel safety.

Section: The organizational level having responsibility for a major functional area of incident management, e.g., Operations, Planning, Logistics, Finance/Administration, and Intelligence (if established). The section is organizationally situated between the Branch and the Incident Command.

Single Resource: An individual, a piece of equipment and its personnel complement, or a crew or team of individuals with an identified work Supervisor that can be used on an incident.

Situation Unit: Functional Unit within the Planning Section responsible for the collection, organization, and analysis of incident status information, and for analysis of the situation as it progresses. Reports to the Planning Section Chief.

Span of Control: The number of individuals a supervisor is responsible for, usually expressed as the ratio of supervisors to individuals. (Under the NIMS, an appropriate span of control is between 1:3 and 1:7.)

Staging Area: Location established where resources can be placed while awaiting a tactical assignment. The Operations Section manages Staging Areas.

Standard Operating Guidelines (SOG): A set of instructions having the force of a directive, covering those features of operations which lend themselves to a definite or standardized procedure without loss of effectiveness.

Standard Operating Procedure (SOP) or Operations Manual: A complete reference document that details the procedures for performing a single function or a number of interdependent functions

State: When capitalized, refers to any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. See Section 2 (14), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Strategic: Strategic elements of incident management are characterized by continuous long-term, high-level planning by organizations headed by elected or other senior officials. These elements involve the adoption of long-range goals and objectives, the setting of priorities; the establishment of budgets and other fiscal decisions, policy development, and the application of measures of performance or effectiveness.

Strategic Objective: A written statement describing an intended outcome; a results-oriented objective.

Strike Team: A set number of resources of the same kind and type that have an established minimum number of personnel.

Strategy: The general direction selected to accomplish incident objectives set by the IC.

Status Reporting: All levels of government initiate status reports (e.g., Situation Reports [SITREPS] and Pollution Reports [POLREPS]) and then disseminate them to other jurisdictions.

Supervisor: The ICS title for individuals responsible for a Division or Group.

Supply Unit: Functional Unit within the Support Branch of the Logistics Section responsible for ordering equipment and supplies required for incident operations.

Supporting Agency: An agency providing support and/or resource assistance to another agency. See also Assisting Agency.

Supporting Technologies: Any technology that may be used to support the NIMS is included in this subsystem. These technologies include orthophoto mapping, remote automatic weather stations, infrared technology, and communications, among various others.

Tactical Objective: A written statement describing an intended output; a product-oriented or productivity-oriented objective. A *tactical objective* describes how a strategic objective will be accomplished. A *tactical objective* describes products that will contribute to achieving a strategic objective.

Task Force: Any combination of resources assembled to support a specific mission or operational need. All resource elements within a Task Force must have common communications and a designated leader.

Technical Assistance: Support provided to State, local, and Tribal jurisdictions when they have the resources but lack the complete knowledge and skills needed to perform a required activity (such as mobile-home park design and hazardous material assessments).

Technical Specialists: Personnel with special skills that can be used anywhere within the ICS organization.

Technology Standards: National standards for key systems may be required to facilitate the interoperability and compatibility of major systems across jurisdictional, geographic, and functional lines.

Technology Support: Facilitates incident operations and sustains the research and development (R&D) programs that underpin the long-term investment in the nation's future incident management capabilities.

Technology Use: Agencies must plan in advance for the effective and efficient use of information management technologies (e.g., computers and networks) to tie together all command, tactical, and support units involved in incident management and to enable these entities to share information critical to mission execution and the cataloguing of required corrective actions.

Terrorism: Under the Homeland Security Act of 2002, terrorism is defined as activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources and is a violation of the criminal laws of the United States or of any State or other subdivision of the United States in which it occurs and is intended to intimidate or coerce the civilian population or influence a government or affect the conduct of a government by mass destruction, assassination, or kidnapping. See Section 2 (15), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Time Unit: Functional Unit within the Finance/Administration Section responsible for recording time for incident personnel and hired equipment.

Threat: An indication of possible violence, harm, or danger.

Tools: Those instruments and capabilities that allow for the professional performance of tasks, such as information systems, agreements, doctrine, capabilities, and legislative authorities.

Tracking and Reporting Resources: Standardized, integrated process conducted throughout the life-cycle of an incident. This process provides incident managers with a clear picture of where resources are located, helps staff prepare to receive resources, protects the safety of personnel and security of supplies and equipment, and enables the coordination of movement of personnel, equipment, and supplies.

Tribal: Any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaskan Native Claims Settlement Act (85 stat. 688) [43 U.S.C.A. and 1601 et seq.], that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

Type: A classification of resources in the ICS that refers to capability. Type 1 is generally considered to be more capable than Types 2, 3, or 4, respectively, because of size; power; capacity; or, in the case of incident management teams, experience and qualifications.

Unified Approach: A major objective of preparedness efforts is to ensure mission integration and interoperability in response to emergent crises across functional and jurisdictional lines, as well as between public and private organizations.

Unified Area Command: A Unified Area Command is established when incidents under an Area Command are multi-jurisdictional. (See Area Command.)

Unified Command: An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP.

Unit: The organizational element having functional responsibility for a specific incident planning, logistics, or finance/administration activity.

Unity of Command: The concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.

Volunteer: For purposes of the NIMS, a volunteer is any individual accepted to perform services by the lead agency, which has authority to accept volunteer services, when the individual performs services without promise, expectation, or receipt of compensation for services performed. See, e.g., 16 U.S.C. 742f(c) and 29 CFR 553.101.

ACRONYMS

AC	Area Command
ALS	Advanced Life Support
DHS	Department of Homeland Security
DOC	Department Operations Center
DOD	Department of Defense
DRC	Disaster Recovery Center
EMAC	Emergency Management Assistance Compact
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
ERT-A	Emergency Response Team-Advance Element
FEMA	Federal Emergency Management Agency
FIN	Finance/Admin Section Chief
FOG	Field Operations Guide
GIS	Geographic Information System
HAZMAT	Hazardous Material
HSPD-5	Homeland Security Presidential Directive-5, Management of Domestic Incidents
HSPD-8	Homeland Security Presidential Directive-8, National Preparedness
IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IC or UC	Incident Command or Unified Command
IMT	Incident Management Team
INS	Incident of National Significance
JFO	Joint Field Office
JIC	Joint Information Center
JIS	Joint Information System
LNO	Liaison Officer
LOG	Logistics Section Chief
MAC	Multi-Agency Coordination Entity
MACS	Multi-Agency Coordination Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NDMS	National Disaster Medical System

NGO	Nongovernmental Organization
NIMS	National Incident Management System
NOC-NRCC	National Operation Center and Response Coordination Center
NRP	National Response Plan
Ops	Operations
P	Press
PAO	Public Affairs Officer
PIO	Public Information Officer
PS	Press Secretary
PSC	Plans Section Chief
PVO	Private Voluntary Organizations
R&D	Research and Development
ROSS	Resource Ordering and Status System
SCO	State Coordinating Office
SDO	Standards Development Organizations
SO	Safety Officer
SOP	Standard Operating Procedure
UAC	Unified Area Command
UC	Unified Command
US&R	Urban Search and Rescue